

## LOGIC BLOG 2016

EDITOR: ANDRÉ NIES

The Logic Blog is for

- rapidly announcing results related to logic
- putting up results and their proofs for further research
- archiving results for later use
- getting feedback before submission to a journal.

Each year's blog is posted on arXiv shortly after the year has ended.

[Logic Blog 2015](#) (Link: <http://arxiv.org/abs/1602.04432>)  
[Logic Blog 2014](#) (Link: <http://arxiv.org/abs/1504.08163>)  
[Logic Blog 2013](#) (Link: <http://arxiv.org/abs/1403.5719>)  
[Logic Blog 2012](#) (Link: <http://arxiv.org/abs/1302.3686>)  
[Logic Blog 2011](#) (Link: <http://arxiv.org/abs/1403.5721>)  
[Logic Blog 2010](#) (Link: <http://dx.doi.org/2292/9821>)

### How does the Logic Blog work?

**Writing and editing.** The source files are in a shared dropbox. Ask André ([andre@cs.auckland.ac.nz](mailto:andre@cs.auckland.ac.nz)) in order to gain access.

**Citing.** Postings can be cited. An example of a citation is:

H. Towsner, *Computability of Ergodic Convergence*. In André Nies (editor), Logic Blog, 2012, Part 1, Section 1, available at <http://arxiv.org/abs/1302.3686>.

**Announcements on the wordpress front end.** The Logic Blog has a [front-end](#) managed by Rupert Hölzl.  
(Link: <http://logicblogfrontend.hoelzl.fr/>)

When you post source code on the logic blog in the dropbox, you can post a comment on the front-end alerting the community, and possibly summarising the result in brief. The front-end is also good for posting questions. It allows MathJax.

The logic blog, once it is on arXiv, produces citations on Google Scholar.

## CONTENTS

<b>Part 1. Randomness, analysis and ergodic theory</b>	<b>3</b>
1. Westrick: randomness and rotations of the unit circle	3
2. Nies: alternative proof of Thm. 1.1 (1)	4
<b>Part 2. Randomness via algorithmic tests</b>	<b>5</b>
3. Smart sets for arbitrary cost functions	5
3.1. The most powerful kind of set obeying a given cost function	5
3.2. ML-reducibility	6
3.3. The strongest cost function obeyed by a given set	7
<b>Part 3. Computability theory</b>	<b>8</b>
4. Merkle, Nies and Stephan: A dual of the Gamma question	8
5. Monin - A resolution of the Gamma question	9
6. Brendle and Nies: Analog for cardinal characteristics of Monin's solution to the $\Gamma$ question	14
7. Nies: answering the $\Delta$ question	19
<b>Part 4. Reverse mathematics</b>	<b>22</b>
8. Belanger, Nies and Shafer: the strength of randomness existence axioms	22
2-randomness versus weak 2-randomness	23
Weak Demuth randomness versus WKL	23
9. Belanger, Nies and Shafer: the strength of randomness existence axioms	24
2-randomness versus weak 2-randomness	25
Weak Demuth randomness versus WKL	25
10. Carlucci: Bounded Hindman's Theorem and Increasing Polarized Ramsey's Theorem	26
Discussion	28
<b>Part 5. Computational complexity theory</b>	<b>29</b>
11. Thompson: Symmetric functions can be computed by Boolean circuits of linear size and logarithmic depth	29
12. Describing ordinals less than $\varepsilon_0$ by finite trees	31
13. Nies and Scholz: Grothendieck's constants	32
<b>Part 6. Group theory and its connections to logic</b>	<b>32</b>
14. Doucha and Nies: Primitive group actions in the setting of Polish Spaces	32
15. Nies and Tent: a sentence of size $O(\log n)$ expressing that a group has $n$ elements	34
16. Melnikov and Nies: A computable compact abelian group such that the Haar measure is not computable	37
17. Fouché and Nies: computable profinite groups	38
17.1. Background on profinite groups	38
17.2. The algorithmic theory	40
18. Rute: On the computability of compact groups	43

<b>Part 7. Metric spaces and descriptive set theory</b>	<b>46</b>
19. Nies and Weiss: complexity of topological isomorphism for subshifts	46
<b>Part 8. Higher computability theory/effective descriptive set theory</b>	<b>47</b>
20. Yu: $\Pi_1^1$ -hyperarithmetic determinacy	47
20.1. Case(1): There is a real $z$ so that $z \in L_{\omega_1^\beta}$ and $\omega_1^z = \omega_1^\beta$ .	49
20.2. Case(2): Otherwise.	49
<b>Part 9. Model theory and definability</b>	<b>54</b>
21. Descriptions in second order logic	54
22. Kolezhitskiy: Robinson's theorem that $\mathbb{Z}$ is definable in $\mathbb{Q}$	55
Idea and structure of the proof	55
Proofs of Lemmas 22.3 and 22.4	56
References	57

## Part 1. Randomness, analysis and ergodic theory

### 1. WESTRICK: RANDOMNESS AND ROTATIONS OF THE UNIT CIRCLE

The following result was obtained at the computability retreat at Research Centre Coromandel in February. It started through discussions between Adam Day, Andre Nies, Dan Turetsky and Brown Westrick.

Let  $P \subseteq [0, 1]$  be a  $\Pi_1^0$  class.

**Theorem 1.1.** *Let  $X \in MLR$ . Let  $k \in \mathbb{N}$ .*

- (1) *There is a rational number  $q \neq 0$  such that for all  $i \leq k$ ,  $X + qi \in P$ .*
- (2) *Let  $\alpha$  be a computable irrational number. There is an integer  $n \neq 0$  such that for all  $i \leq k$ ,  $(X + \alpha ni \bmod 1) \in P$ .*

*Proof.* Both (1) and (2) are proved by the same method. Dynamically construct a Solovay test as follows. Put the empty string  $\langle \rangle$  in the test. Then for any  $\sigma$  that has been placed in the test, let  $r_\sigma$  be a rational number (for (1)) or let  $n_\sigma > 0$  be an integer (for (2)) such that

$$\frac{2^{-|\sigma|}}{2k+3} < r_\sigma, (\alpha n_\sigma \bmod 1) < \frac{2^{-|\sigma|}}{2k+2}.$$

These bounds are chosen so that for every  $z \in [\sigma]$ ,  $z + kr_\sigma \in [\sigma]$  or  $z - kr_\sigma \in [\sigma]$ . Let  $U_s$  denote the complement of  $P$  as seen at stage  $s$ . We will enumerate  $\tau$  into the test at stage  $s$  if we see the following occur:

- (1)  $\sigma \prec \tau$ ,
- (2)  $\tau$  is incomparable with any  $\tau'$  which has already entered the test on the basis of this same  $\sigma$
- (3)  $[\tau] \cap U_s = \emptyset$
- (4) For some integer  $i \in [-k, k]$ ,  $[\tau] + ir_\sigma \subseteq [\sigma] \cap U_s$ .

The point is to enumerate  $[\tau]$  if its potential  $\pm r_\sigma$   $k$ -recurrence inside  $[\sigma]$  is invalidated. For (2), replace  $r_\sigma$  everywhere with  $\alpha n_\sigma \bmod 1$ .

The test catches any  $z \in P$  which fails to  $k$ -recur for all  $r \in \mathbb{Q} \setminus \{0\}$  (resp. for all  $\alpha n$  with  $n \in \mathbb{Z} \setminus \{0\}$ ). We need to show it is a Solovay test.

We show that for every  $\sigma$  in the test, the total measure of all  $\tau$  added to the test as a result of  $\sigma$  is at most  $\frac{2k+2}{2k+3}\mu[\sigma]$ . So if the depth of  $\tau$  is the number of initial segments that  $\tau$  has in the test, then  $\mu(\cup\{\tau\} : \tau \text{ of depth } d\}) \leq \left(\frac{2k+2}{2k+3}\right)^d$ , so this will suffice to show that the total measure of the test is finite.

When  $\sigma$  is first put in the test,  $[\sigma]$  is disjoint from  $U_s$ . When first  $\rho$  enters  $U_s$  with  $\sigma \prec \rho$ , we can consider  $[\sigma]$  as being divided into two parts, both invariant under addition of  $r_\sigma$ :  $C = \{z \in [\sigma] : z + ir_\sigma \in [\rho] \text{ for some } i \in \mathbb{Z}\}$ , and its complement. All  $z$  whose initial segments could potentially be enumerated as a result of  $\rho$  are contained in  $C$ . Also  $[\rho] \subseteq C$ , but nothing comparable with  $\rho$  will be enumerated. By the choice of  $r_\sigma$ ,  $\frac{\mu[\rho]}{\mu C} \leq \frac{1}{2k+3}$ . Therefore, the measure added to the test as a result of the addition of  $\rho$ , and as a result of the addition of any future  $\rho'$  with  $[\rho'] \subseteq C$ , is bounded by  $\frac{2k+2}{2k+3}\mu C$ .

The remaining set  $[\sigma] \setminus C$  is currently untouched but may in the future be seen to intersect the complement of  $P$ . When that happens, we apply the same reasoning inside of  $[\sigma] \setminus C$ , partitioning it into two invariant pieces and arguing that one piece remains untouched, while the other can never contribute more than  $\frac{2k+2}{2k+3}$  of its measure to the test. Continuing in this way, we get the desired bound on the measure the test uses in response to  $\sigma$ .  $\square$

## 2. NIES: ALTERNATIVE PROOF OF THM. 1.1 (1)

The case  $k = 1$  of the theorem can be derived from a result of Figueira et al. [14]; also see [31, 3.3.7]. That theorem of [14] says that if  $X$  is not autoreducible, then there is a bit position  $n$  such that the bit  $n$  is indifferent for  $X$  with respect to  $P$ , which means that we can change  $X$  at  $n$  and remain in  $P$ . This change corresponds to adding or subtracting the rational  $2^{-n}$ .

Now let us obtain an arithmetical progression namely  $X + qi \in P$  for  $i < k/2$  (for technical reasons).

At first we work with  $Z \in k^\omega$ . Extending the case of  $k = 2$ , we say that  $Z$  is auto-reducible if there is a reduction procedure  $\Phi$  such that  $\Phi^Z(n) \neq Z(n)$  for each  $n$ , and the computation  $\Phi^Z(n)$  only queries the oracle at values other than  $n$ . As before, one checks that a ML-random sequence  $Z$  is not auto-reducible. We say that position  $n$  is indifferent for  $Z$  with respect to a  $\Pi_1^0$  class  $P \subseteq k^\omega$  if we can change  $Z$  at  $n$  to any value  $< k$  and remain in  $P$ .

**Proposition 2.1.** *Let  $Q \subseteq k^\omega$  be a  $\Pi_1^0$  class. If  $Z \in Q$  is not autoreducible, then there is a position  $n$  such that the bit  $n$  is indifferent for  $Z$  with respect to  $Q$ .*

*Proof.* A straightforward extension of the argument for  $k = 2$ . If there is no such position, given input  $n$  the reduction  $\Phi$  searches for a stage  $s$  and  $i < k$  such that  $Z$ , with position  $n$  changed to value  $i$ , is not in  $Q$ , and once found, output this  $i$ .  $\square$

To obtain the arithmetical progression assume that  $k = 2^r$  for  $r \in \mathbb{N}$ . Given  $\Pi_1^0$  class  $P \subseteq 2^\mathbb{N}$  and ML-random  $X \in P$ , let  $Q, Z$  be the

class/sequence rewritten using the alphabet  $0, \dots, k-1$ . That is, the block bits of  $X$  in positions  $nr \dots (n+1)r - 1$  corresponds the symbol of  $Z$  in position  $n$ . If  $n$  is indifferent for  $Z$  in  $Q$ , then we have an arithmetical progression  $X + qi \in P$ , where  $i < k/2$ ,  $q = \pm 2^{-rn}$ .

## Part 2. Randomness via algorithmic tests

### 3. SMART SETS FOR ARBITRARY COST FUNCTIONS

The following is work of Greenberg, Miller, Nies and Turetsky at RCC in Feb. 2015, and in Wellington slightly later. For background on cost functions see [30]. In the following all cost functions satisfy the limit condition  $\lim_x \mathbf{c}(x) = 0$ .

**Definition 3.1** ([3]). Let  $\mathbf{c}$  be a cost function. A descending sequence  $\langle V_n \rangle$  of uniformly c.e. open sets is a  $\mathbf{c}$ -bounded test if  $\lambda(V_n) = O(\mathbf{c}(n))$  for all  $n$ .

We think of each  $V_n$  as an approximation for  $Y \in \bigcap_k V_k$ . Being in  $\bigcap_n V_n$  can be viewed as a new sense of obeying  $\mathbf{c}$  that makes sense for ML-random sets.

**Lemma 3.2.** Suppose  $aY$  fails a  $\mathbf{c}$ -bounded test  $\bigcap_n V_n$  where  $a \in \{0, 1\}$ . Then  $Y$  fails a  $\mathbf{c}$ -bounded test.

*Proof.* We may suppose  $a = 0$  and  $X \in V_n$  implies  $X(0) = 0$ . Since  $\lambda T(V_n) \leq 2\lambda V_n$  where  $T$  is the usual shift operator on Cantor space,  $\langle T(V_n) \rangle$  is also a  $\mathbf{c}$ -bounded test. Clearly  $Y$  fails it.  $\square$

The basic motivating result is a generalisation in terms of cost functions of a fact of Hirschfeldt and Miller.

**Proposition 3.3.** If  $A \models \mathbf{c}$  and  $Y$  is a ML-random captured by a  $\mathbf{c}$ -bounded test, then  $A \leq_T Y$ .

#### 3.1. The most powerful kind of set obeying a given cost function.

The following is the central definition for this entry: given  $\mathbf{c}$ , we consider sets  $A$  such that the converse implication holds as well.

**Definition 3.4.** Let  $\mathbf{c}$  be a cost function and  $A$  be a  $\Delta_2^0$  set. We say that  $A$  is *smart for  $\mathbf{c}$*  if  $A \models \mathbf{c}$  and for each ML-random set  $Y$ ,

$$Y \text{ is captured by a } \mathbf{c}\text{-bounded test} \Leftrightarrow A \leq_T Y.$$

Informally, if  $A$  is smart for  $\mathbf{c}$  then  $A$  is as complex as possible among the sets obeying  $\mathbf{c}$ , in the sense that the only random sets  $Y$  above  $A$  are the ones that have to be there because  $A$  obeys the cost function that puts it below  $Y$  anyway.

**Theorem 3.5.** Let  $\mathbf{c}$  be a cost function with  $\mathbf{c} \rightarrow \mathbf{c}_\Omega$ . Some c.e. set  $A$  is smart for  $\mathbf{c}$ .

*Proof.* Recall  $\Upsilon$  is a “universal” Turing functional in the sense that  $\Upsilon(0^e 1^\infty X) = \Phi_e(X)$  for each  $X, e$ . We build  $A$  and a  $\mathbf{c}$ -test  $\langle \mathcal{U}_k \rangle$  capturing any ML-random  $Y$  such that  $A = \Upsilon^Y$ . This suffices for the theorem by Lemma 3.2.

Since  $2^{-x} \leq^\times \Omega - \Omega_x$ , we may assume that  $\mathbf{c}(x, s) \geq 2^{-x}$  for  $x \leq s$ .

As in [3], during the construction of  $A$  we build a global “error set”:

$$\mathcal{E}_s = \{Y : \exists n [\Upsilon_s^Y(n) \downarrow = 0 \wedge A_s(n) = 1]\}$$

All all stages  $s$  we will have

$$(\diamond) \quad \lambda \mathcal{U}_{k,s} \leq \mathbf{c}(k, s) + \lambda(\mathcal{E}_{s+1} - \mathcal{E}_k).$$

So since  $\lambda(\mathcal{E} - \mathcal{E}_k) \leq^\times \mathbf{c}_\Omega(k)$  and  $\mathbf{c}_\Omega(k) \leq^\times \underline{\mathbf{c}}(k)$ , the test  $\langle \mathcal{U}_k \rangle$  is indeed a  $\mathbf{c}$ -test.

We reserve the interval  $I_k = [2^k, 2^{k+1})$  for ensuring  $(\diamond)$ . The construction of  $\mathcal{U}_k$  is as follows. At stage  $s > k$ , let  $x = \min(I_k - A_{s-1})$ . Let

$$\mathcal{U}_{k,s} = \bigcup_{t < s} \{Y : A_t \upharpoonright_{x+1} \preceq \Upsilon_t^Y\} - \mathcal{E}_k$$

If  $(\diamond)$  threatens to fail at  $s$ , namely  $\lambda \mathcal{U}_{k,s} > \mathbf{c}(k, s) + \lambda(\mathcal{E}_s - \mathcal{E}_k)$ , put  $x$  into  $A_{s+1}$ . This causes  $\mathcal{U}_{k,s}$  to go into  $\mathcal{E}_{s+1}$ .

First we verify that  $x$  always exists, that is, we enumerate at most  $2^k$  times for  $\mathcal{U}_k$ . If we do this at stage  $s$ ,  $\lambda \mathcal{U}_{k,s} > 2^{-k} + \lambda(\mathcal{E}_s - \mathcal{E}_k)$ . Since  $\mathcal{U}_{k,s} \cap \mathcal{E}_k = \emptyset$  by definition, and  $\mathcal{U}_{k,s} \subseteq \mathcal{E}_{s+1}$ , it follows that  $\lambda(\mathcal{E}_{s+1} - \mathcal{E}_s) > 2^{-k}$ . Since  $\lambda \mathcal{E} \leq 1$ , this can happen at most  $2^k$  times.

In particular, if  $A = \Upsilon^Z$  then  $Z \in \bigcap_k \mathcal{U}_k$ .

It remains to verify that  $A \models \mathbf{c}$ . If we enumerate  $x$  for  $\mathcal{U}_k$  at stage  $s$  then  $\lambda(\mathcal{U}_{k,s} - \mathcal{E}_s) = \lambda(\mathcal{U}_{k,s} - (\mathcal{E}_s - \mathcal{E}_k)) \geq \lambda(\mathcal{U}_{k,s}) - \lambda(\mathcal{E}_s - \mathcal{E}_k) > \mathbf{c}(k, s) \geq \mathbf{c}(x, s)$ . Since  $\mathcal{U}_{k,s} - \mathcal{E}_s \subseteq \mathcal{E}_{s+1} - \mathcal{E}_s$ , we see that  $\mathbf{c}(x, s) < \lambda(\mathcal{E}_{s+1} - \mathcal{E}_s)$ . This implies that the total cost of the enumeration of  $A$  is at most 1.  $\square$

### 3.2. ML-reducibility.

**Definition 3.6** ([3]). For  $K$ -trivial sets  $A$  and  $B$ , we write  $B \leq_{\text{ML}} A$  if  $A \leq_{\text{T}} Y$  implies  $B \leq_{\text{T}} Y$  for any ML-random set  $Y$ .

Clearly,  $\leq_{\text{T}}$  implies  $\leq_{\text{ML}}$ . The ML-degrees form an upper semilattice where the least upper bound of  $K$ -trivial sets  $C$  and  $D$  is given by the  $K$ -trivial set  $C \oplus D$ .

**Definition 3.7.** Let  $\mathbf{c}$  be a cost function and  $A$  be a  $\Delta_2^0$  set. We say that  $A$  is *ML-complete for  $\mathbf{c}$*  if  $A \models \mathbf{c}$ , and  $\forall B [B \models \mathbf{c} \Rightarrow B \leq_{\text{ML}} A]$ .

**Corollary 3.8.**  $A$  is smart for  $\mathbf{c} \Leftrightarrow A$  is ML-complete for  $\mathbf{c}$ .

*Proof.*  $\Rightarrow$ : Suppose  $A \leq_{\text{T}} Y$  for ML-random  $Y$ . Then some  $\mathbf{c}$ -bounded test captures  $Y$ . If  $B \models \mathbf{c}$ , then  $B \leq_{\text{T}} Y$  by the basic fact 3.3. Thus  $B \leq_{\text{ML}} A$  as required.

$\Leftarrow$ : By Theorem 3.5 let  $\tilde{A}$  be smart for  $\mathbf{c}$ . Suppose  $A \leq_{\text{T}} Y$  for ML-random  $Y$ ; we want to show that  $Y$  is captured by a  $\mathbf{c}$ -bounded test. Since  $A$  is ML-complete for  $\mathbf{c}$  we have  $\tilde{A} \leq_{\text{ML}} A$ , so  $\tilde{A} \leq_{\text{T}} Y$ , so  $Y$  is captured by a  $\mathbf{c}$ -bounded test as required.  $\square$

In particular, the ML-degree of a smart set  $A$  for  $\mathbf{c}$  is uniquely determined by  $\mathbf{c}$ . On the other hand, for each low c.e. set  $A$  there is a c.e. set  $B \not\leq_{\text{T}} A$  such that  $B \models \mathbf{c}$  [31, 5.3.22]. If  $A$  is smart for  $\mathbf{c}$ , then  $A \oplus B$  is also smart for  $\mathbf{c}$ . As each  $K$ -trivial is low, the Turing degree of a set  $A$  that is smart for  $\mathbf{c}$  is not uniquely determined by  $\mathbf{c}$ .

**Question 3.9.** *Given  $\mathbf{c}$  can we build a smart for  $\mathbf{c}$  set  $A$  that is cappable? Can we even have two smart for  $\mathbf{c}$  sets that form a minimal pair?*

**3.3. The strongest cost function obeyed by a given set.** Given c.e.  $K$ -trivial  $A$  we will define a c.f.  $\mathbf{c}_A$  with  $A \models \mathbf{c}_A$  such that every random computing  $A$  is captured by a  $\mathbf{c}_A$  test. (In other words,  $A$  is smart for  $\mathbf{c}_A$ .) However,  $\mathbf{c}_A$  may not be a very natural cost function. We build a  $K$ -trivial  $A$  such that the class of sets obeying  $\mathbf{c}_A$  is not closed downward under  $\leq_T$ , and in fact not even the shift  $T(A)$  obeys  $\mathbf{c}_A$ .

As before  $\Upsilon$  denotes a “universal” Turing functional. Given a c.e.  $K$ -trivial set  $A$ , fix a c.e. approximation  $\langle A_s \rangle \models \mathbf{c}_\Omega$ . We let

$$\mathbf{c}_A(x, s) = \lambda \bigcup_{x \leq t < s} \{Y : A_t \upharpoonright_{x+1} \preceq \Upsilon_t^Y\}.$$

**Proposition 3.10.** (i)  $A \models \mathbf{c}_A$ . (ii) Suppose  $\mathbf{c}$  is a cost function such that  $A \models \mathbf{c}$ . Then  $\mathbf{c}_A \rightarrow \mathbf{c}$ . In particular,  $\mathbf{c}_A \rightarrow \mathbf{c}_\Omega$ .

*Proof.* (i) We show that the fixed approximation  $\langle A_s \rangle \models \mathbf{c}_A$ . Define the left-c.e. “error real” by:

$$\epsilon_s = \lambda \{Y : \exists n [\Upsilon_s^Y(n) \downarrow = 0 \wedge A_s(n) = 1]\}$$

Note that if  $x \in A_s - A_{s-1}$ , then  $\mathbf{c}_A(x, s) \leq \epsilon_s - \epsilon_x = \mathbf{c}_\epsilon(x, s)$ . So  $\mathbf{c}_A \langle A_s \rangle \leq \mathbf{c}_\epsilon \langle A_s \rangle$ . Since  $\mathbf{c}_\Omega \rightarrow \mathbf{c}_\epsilon$ , and  $\langle A_s \rangle \models \mathbf{c}_\Omega$ , it follows that  $\langle A_s \rangle \models \mathbf{c}_A$ .

(ii) By multiplying by a constant, we may assume that  $\mathbf{c}(0) < 1/2$ . Fix a computable speed-up  $f$  such that  $\mathbf{c} \langle A_{f(s)} \rangle < 1/2$ . Define a Turing functional  $\Psi$  such that at every stage  $f(s)$ ,  $\lambda \{Y : A_{f(s)} \upharpoonright_{x+1} \prec \Psi_{f(s)}^Y\} = \mathbf{c}(x, s)$ . By a simple argument, the measure of the error-set  $\mathcal{E}$  for this functional will be  $\mathbf{c} \langle A_{f(s)} \rangle < 1/2$ , so this construction may proceed.

Fix  $e$  with  $\Phi_e = \Psi$ . Then  $\mathbf{c}_A(x) \geq 2^{-(e+1)} \mathbf{c}_\epsilon(x)$ . □

Recall that  $T(A)$  is the shift of  $A$ .

**Theorem 3.11.** *For each cost function  $\mathbf{d}$ , there is a cost function  $\mathbf{c} \geq \mathbf{d}$  and a c.e. set  $A$  such that  $A \models \mathbf{c}$  and  $T(A) \not\models \mathbf{c}$ .*

Since  $\mathbf{c}_A \rightarrow \mathbf{c}$ , this shows that  $T(A) \not\models \mathbf{c}_A$ .

*Proof.* We fix a listing  $\langle \Phi_e \rangle$  of all (possibly partial) computable enumerations  $\langle B_t \rangle$ , where  $B_t \simeq D_{\Phi_e(t)}$  and  $D_{\Phi_e(t)} \subseteq D_{\Phi_e(t+1)}$  if defined.

We may assume  $\mathbf{d}(s-1, s) \geq 2^{-s}$ . We define  $\mathbf{c}(x, s)$  so that  $\mathbf{c}(x, s) \geq \mathbf{d}(x, s)$  for each  $x, s$ . At a stage  $x$  of the construction we may also declare that  $\mathbf{c}(x-1, x) \geq \alpha$ , which by monotonicity entails that  $\mathbf{c}(y, s) \geq \alpha$  for each  $y < x$  and  $s \geq x$ .

We meet the requirements

$$R_e : T(A) = \bigcup_t D_{\Phi_e(t)} \Rightarrow \mathbf{c} \langle \Phi_e \rangle \geq 1.$$

The strategy for  $R_e$  tries to ensure  $\mathbf{c}(x-1)$  is large and  $\mathbf{c}(x)$  is small for sufficiently many  $x$ . In that case  $R_e$  can put  $x$  into  $A$  for the small cost, while the opponent’s enumeration  $\langle \Phi_e \rangle$  of  $T(A)$  has to deal with the large cost. One problems in implementing this idea is the timing as we will of  $\Phi_e(u)$  for a stage  $u$  only at a stage  $s$  much larger than  $u$ . Also we always have

$\mathbf{c}(x, s) \geq \mathbf{d}(x, s)$ , so once we discover that the enumeration of  $x$  would help because  $\langle \Phi_e \rangle$  caught up sufficiently much, it may be that the enumeration of  $x$  has become too expensive for  $R_e$ . Similar to the usual construction of a set obeying  $\mathbf{d}$ , in this case we simply pick a new  $x$ . Since  $\mathbf{d}$  has the limit condition, eventually we will always be able to keep  $x$ .

At a stage  $s > 0$  let  $s_{\text{init}}(e)$  be the greatest stage  $t < s$  such that  $t = 0$  or  $R_e$  has been initialised at  $t$ . If by stage  $s$  the strategy for  $R_e$  has been initialised for  $b$  times it can spend a  $\mathbf{c}$ -cost of  $2^{-b-e}$  in enumerating  $A$ . It is also allowed to raise  $\mathbf{c}(x, s)$  to  $2^{-s_{\text{init}}(e)}$ .

The  $e$ -expansionary stages are the ones at which  $\langle \Phi_e \rangle$  catches up with  $T(A)$ . We declare 0 as  $e$ -expansionary. A stage  $s > 0$  is  $e$ -expansionary if for the largest  $e$ -expansionary stage  $t < s$ , we have that  $T(A_s) \upharpoonright_{t+2} = \Phi_{e,s}(u) \upharpoonright_{t+2}$  where  $u$  is largest such that  $\Phi_{e,s}(u)$  is defined and  $u > t$ .

*Strategy for  $R_e$ .* Write  $\alpha = 2^{-s_{\text{init}}(e)}$ . A rational parameter  $\gamma_e \in [0, 1]$  measures progress of  $R_e$ . We set  $\gamma_e$  to 0 when  $R_e$  is initialised.

At  $e$ -expansionary stage  $s$ , if  $\gamma_e \leq 1$  do the following. Initialize lower priority requirements. Declare that  $\mathbf{c}(s-1, s+1) \geq \alpha$ . (So for  $\Phi_e$ , changing at  $s-1$  will be expensive after stage  $s$ .)

Let  $x < s$  be the last  $e$ -expansionary stage. If  $\mathbf{d}(x, s) < 2^{-b-e}\alpha$ , put  $x$  into  $A_s$  (note that no-one has raised the  $\mathbf{c}$  cost for  $x$  above  $\mathbf{d}(x, s)$  yet), add  $\alpha$  to  $\gamma_e$ . Say that  $R_e$  acts.

Clearly  $R_e$  only acts  $2^{s_{\text{init}}(e)} = 1/\alpha$  times while it is not initialised.

**Claim 3.12.**  $A \models \mathbf{c}$ .

When  $R_e$  acts at  $s$  we have  $\mathbf{c}(x, s) \leq 2^{-b-e}\alpha$  by initialisation.

**Claim 3.13.**  $TA \not\models \mathbf{c}$ .

Otherwise  $TA \models \mathbf{c}$  via some enumeration  $\langle \Phi_e \rangle$  such that  $\mathbf{c}(\Phi_e) < 1$ . Since  $\mathbf{d}$  satisfies the limit condition,  $\gamma_e$  reaches the value 1. This is at least what  $\langle \Phi_e \rangle$  pays for the enumerations of  $x-1$  into  $TA$ . For when  $R_e$  acts at  $s$  via  $x$  then  $x-1 \notin \Phi_e(u)$  for some  $u > x$  since  $s$  is  $e$ -expansionary. By the next  $e$ -expansionary stage we have  $x-1 \in \Phi_e(u')$  for some  $u' > u$ . So  $\Phi_e$  paid the cost  $\mathbf{c}(x-1, x+1) \geq \alpha$  that was set by  $R_e$  at stage  $x$ .  $\square$

### Part 3. Computability theory

#### 4. MERKLE, NIES AND STEPHAN: A DUAL OF THE GAMMA QUESTION

Merkle, Nies and Stephan worked at NUS in February. They considered a dual of the  $\Gamma$  operator on Turing degrees.

For  $Z \subseteq \mathbb{N}$  the lower density is defined to be

$$\underline{\rho}(Z) = \liminf_n \frac{|Z \cap [0, n)|}{n}.$$

Recall that

$$\gamma(A) = \sup_{X \text{ computable}} \underline{\rho}(A \leftrightarrow X)$$

$$\Gamma(A) = \inf\{\gamma(Y) : Y \leq_T A\}$$

which only depends on the Turing degree of  $A$ . The  $\Gamma$  operator was introduced by Andrews, Cai, Diamondstone, Jockusch and Lempp [1].



**Definition 4.1.**

$$\delta(A) = \inf_{X \text{ computable}} \rho(A \leftrightarrow X)$$

$$\Delta(A) = \sup\{\delta(Y) : Y \leq_T A\}.$$

Intuitively,

- $\Gamma(A)$  measures how well computable sets can approximate the sets that  $A$  computes, counting the asymptotically worst case (the infimum over all  $Y \leq_T A$ ). In contrast,
- $\Delta(A)$  measures how well the sets that  $A$  computes can approximate the computable sets, counting the asymptotically best case (the supremum over all  $Y \leq_T A$ ).

Clearly the maximum value of  $\Delta(A)$  is  $1/2$ . The operator  $\Delta(A)$  is related to the analog of a cardinal characteristic introduced by Brendle and Nies in the 2015 Logic Blog [12]. They define  $\mathcal{B}(\sim_p)$  to be the class of oracles  $A$  that compute a set  $Y$  such that for each computable set  $X$ , we have  $\rho(X \leftrightarrow Y) > p$ . For each  $p$  with  $0 \leq p < 1/2$ ,

$$\Delta(A) > p \Rightarrow A \in \mathcal{B}(\sim_p) \Rightarrow \Delta(A) \geq p.$$

We state three minor results.

**Proposition 4.2.** *Let  $A$  be 2-generic. Then  $\Delta(A) = 0$ .*

A proof is given at the end of Section 7.

**Proposition 4.3.** *Let  $A$  compute a Schnorr random  $Y$ . Then  $\Delta(A) = 1/2$ .*

This is clear because  $\rho(Y \leftrightarrow R) = 1/2$  for each computable  $R$ .

**Proposition 4.4.** *Let  $p \in (0, 1/2)$  be computable. Let  $A$  be Schnorr random for the Bernoulli measure w.r.t.  $p$ . Then  $\delta(B) = p$  for each  $B \equiv_1 A$ .*

The “ $\Delta$ -question” is (or rather, was, and has been quite short-lived):

**Question 4.5** (solved). *Can  $\Delta(A)$  be properly between 0 and  $1/2$ ?*

Using a dual form of Monin’s technique’s below, this has been answered in the negative by Nies; see Section 7.

## 5. MONIN - A RESOLUTION OF THE GAMMA QUESTION

We show that there is no sequence  $X$  with a Gamma value strictly between 0 and  $1/2$ .

**Definition 5.1.** For a given  $n \in \omega$  and two strings  $\sigma_1, \sigma_2 \in 2^n$ , the notation  $d(\sigma_1, \sigma_2)$  denotes the normalised **hamming distance** between  $\sigma_1$  and  $\sigma_2$ , that is, the number of bits on which  $\sigma_1$  and  $\sigma_2$  differ divided by  $n$ .

**Definition 5.2.** Let  $F : \omega \rightarrow \omega$  be a function. Given a function  $f$  such that  $f(n) < 2^{F(n)}$ , for each  $n$ , by  $[f(n)]$  we denote the string of length  $F(n)$  encoded by  $f(n)$ .

The following weakens the notion of infinitely often equal (i.o.e.) for a computable bound, which was first studied in [29].

**Definition 5.3.** Let  $F : \omega \rightarrow \omega$  be a function and  $\alpha \in [0, 1]$ . A function  $f$  is  $2^{F(n)}$ -infinitely often  $\alpha$ -equal if for every computable function  $g : \omega \rightarrow \omega$  which is bounded by  $2^{F(n)}$ , we have:

$$\liminf_n d([f(n)], [g(n)]) \leq 1 - \alpha$$

Informally, we want  $f$  to equal infinitely often on a fraction of at least  $\alpha$  bits, to every computable function bounded by  $2^{F(n)}$ . Typically we will have  $\alpha > 1/2$ .

**Proposition 5.4.** Let  $1/2 < \alpha < 1$ . Suppose that for no  $k$ ,  $X$  computes a function which is  $2^{\lfloor 2^{n/k} \rfloor}$ -i.o. $\alpha$ -e. Then  $\Gamma(X) \geq 1 - \alpha$ .

*Proof.* Consider any sequence  $Y$  computed by  $X$ . Fix some  $c \in \omega$  and let  $k$  be the smallest integer such that  $2^{1/k} - 1 < 1/(2c)$ . We then split  $Y$  in blocks of bits of length  $\lfloor 2^{n/k} \rfloor$ . We now argue that for  $n$  large enough, the number of bits in the  $n + 1$ -th block is smaller than  $1/c$  times the sum of the number of bits in the previous blocks. By the sum of geometric series we have:

$$\sum_{i=0}^{i \leq n} 2^{i/k} = \frac{2^{(n+1)/k} - 1}{2^{1/k} - 1}$$

which implies that

$$\begin{aligned} 2^{(n+1)/k} - 1 &= (2^{1/k} - 1) \sum_{i=0}^{i \leq n} 2^{i/k} \\ &\leq \frac{1}{2c} \sum_{i=0}^{i \leq n} 2^{i/k} \end{aligned}$$

For  $n$  large enough we have  $\frac{1}{2} \sum_{i=0}^{i \leq n} 2^{i/k} > (n + c)$ . Thus for  $n$  large enough we have:

$$\begin{aligned} 2^{(n+1)/k} - 1 &\leq \frac{1}{2c} \sum_{i=0}^{i \leq n} 2^{i/k} \\ &\leq \frac{1}{2c} \sum_{i=0}^{i \leq n} 2^{i/k} + \frac{1}{2c} \sum_{i=0}^{i \leq n} 2^{i/k} - \frac{1}{c}(n + c) \\ &\leq \frac{1}{c} (\sum_{i=0}^{i \leq n} 2^{i/k} - n - c) \\ &\leq \frac{1}{c} (\sum_{i=0}^{i \leq n} \lfloor 2^{i/k} \rfloor - c) \\ &\leq \frac{1}{c} (\sum_{i=0}^{i \leq n} \lfloor 2^{i/k} \rfloor) - 1 \end{aligned}$$

We then have for  $n$  large enough that:

$$\lfloor 2^{(n+1)/k} \rfloor \leq \frac{1}{c} \left( \sum_{i=0}^{i \leq n} \lfloor 2^{i/k} \rfloor \right)$$

Thus the length of the  $n + 1$  block of bit is smaller than  $1/c$  of the sum of the length of the previous blocks.

Define the function  $f < 2^{\lfloor 2^{n/k} \rfloor}$  by setting  $f(n)$  to the value coded by the bits of the  $n$ -th block. Suppose that  $f$  is not  $2^{\lfloor 2^{n/k} \rfloor}$  i.o. $\alpha$ -e. In particular there must be some computable function  $h \leq 2^{\lfloor 2^{n/k} \rfloor}$  such that for almost every  $n$ ,  $[h(n)]$  agrees with  $[f(n)]$  on a fraction of strictly less than  $\alpha$  bits. Let  $h'$  be defined as the complement of  $h$  bitwise. Then for almost every  $n$ ,  $[h'(n)]$  agrees with  $[f(n)]$  on a fraction of bits strictly bigger than  $1 - \alpha$ .

Now consider the bit number  $m$  of the sequence defined by  $f$ , starting at the begining of a block. Let  $m + n$  be the last position of that block. By

hypothesis, among the  $m$  first bits (for  $m$  large enough), there are at least  $m(1 - \alpha) - \mathcal{O}(1)$  bits which are guessed correctly by  $h'$ . In particular, for any  $1 \leq i \leq n$ , there are also at least  $m(1 - \alpha) - \mathcal{O}(1)$  bits which are guessed correctly among the  $m + i$  first bits. Also for any  $1 \leq i \leq n$ , the number of total bits is at most  $m + n$ , which is at most  $m + m/c$ . Thus for each  $i$  the fraction of bits which are guessed correctly before  $m + i$  is at least:

$$\frac{m(1 - \alpha) - \mathcal{O}(1)}{m + m/c}$$

As  $m$  goes to infinity, this value converges to:

$$\frac{1 - \alpha}{1 + 1/c}$$

Thus  $\gamma(Y) \geq \frac{1 - \alpha}{1 + 1/c}$ . We can carry out this argument for  $c$  larger and larger, making lower bounds on  $\gamma(Y)$  closer and closer to  $1 - \alpha$ . Thus if for any  $k$ , we can split any  $Y$  into blocks of bits as above such that the resulting function is not  $2^{\lfloor 2^{n/k} \rfloor}$ -i.o. $\alpha$ -e., then  $\gamma(Y) \geq 1 - \alpha$ . By hypothesis we can do this for every  $Y$  computable by  $X$ . Hence  $\Gamma(X) \geq 1 - \alpha$ .  $\square$

By contrapositive, if  $\Gamma(X) < (1 - \alpha)$ , for  $1/2 < \alpha < 1$ , then for some  $k \in \omega$ ,  $X$  computes a function which is  $2^{\lfloor 2^{n/k} \rfloor}$ -i.o. $\alpha$ -e.

We now need to borrow some technics from the field of error correcting codes. The idea is the folloing: We want to transmit some message of length  $m$ . But some random bit flip can occur during the transmission. We want to make sure that if the percentage of error is small enough, we can still recover the original message. The idea is to use an injection  $\Phi$  from  $2^m$  into  $2^n$  for some  $n \gg m$ , in such a way that the elements in the range of  $\Phi$ , are pairwise far away from each other, in the sense of the hamming distance. If  $d$  is the smallest distance between two elements in the range of  $\Phi$ , then it is clear that we can recover up to  $d/2$  error.

Also we would like  $n$  to be not much bigger than  $m$  (ideally a multiplicative constant). It is easy to find such a multiplicative constant allowing, to have a list of  $2^m$  elements of  $2^n$ , which are all at a distance of at least  $1/2 - \epsilon$  from each other, for  $\epsilon$  as small as we want. Thus it is possible to correct this way, up to a fraction  $1/4$  of error. It is not anymore possible if the fraction is bigger than  $1/4$ . However, if the fraction is smaller than  $1/2$ , it is possible to identify a small list of messages, among which must figure our original message. It is even possible to make the size of the list constant. Formally we use the following theorem, for which we provide a proof for completeness:

**Theorem 5.5** (The list decoding capacity theorem). *Let  $0 < \theta < 1/2$ . There exists  $L \in \omega$  and  $0 < R < 1$  as follows.*

*For any  $n$ , there exists a set  $C$  of  $2^{\lfloor Rn \rfloor}$  many strings of length  $n$  such that for any string  $\sigma$  of length  $n$ , there are at most  $L$  strings  $\tau$  in  $C$  such that  $d(\sigma, \tau) < \theta$ .*

*Proof.* We prove that for parameters  $L$  and  $R$  well chosen, if we pick at random the strings in  $C$ , the theorem is true with positive probability.

Let  $\beta = 2(1/2 - \theta)^2 \log(e)$  and pick  $L$  such that  $\beta - \frac{1}{L} > 0$ . Then pick  $R$  such that  $R < \beta - \frac{1}{L}$ .

Using Chernoff bounds, for any string  $\tau$  of length  $n$ , the measure of the set  $\{[\sigma] : |\sigma| = n \text{ and } d(\tau, \sigma) < \theta\}$  is bounded by  $e^{-2(1/2-\theta)^2 n} = 2^{-\beta n}$ . Thus, given a string  $\sigma$  the probability that picking a string  $\tau$  at random gives  $d(\sigma, \tau) < \theta$ , is bounded by  $2^{-\beta n}$ .

Now let  $q = \lfloor Rn \rfloor$  and let  $C$  be a collection of  $2^q$  strings picked at random. For any subset of  $L + 1$  of these strings, the probability that a given string  $\sigma$  has a hamming distance smaller than  $\theta$  with each of them is bounded by  $2^{-\beta n(L+1)}$ . Thus the probability that a given  $\sigma$  has a hamming distance smaller than  $\theta$  with any possible subsets of size  $L + 1$  of  $C$  is bounded by  $\binom{2^q}{L+1} 2^{-\beta n(L+1)}$ . And the probability that this happens for any string  $\sigma$  is bounded by  $2^n \binom{2^q}{L+1} 2^{-\beta n(L+1)}$ . The following computation shows that this quantity is smaller than 1:

$$\begin{aligned} 2^n \binom{2^q}{L+1} 2^{-\beta n(L+1)} &\leq 2^n 2^{Rn(L+1)} 2^{-\beta n(L+1)} \\ &\leq 2^{-n(L+1)(-R-1/(L+1)+\beta)} \\ &\leq 2^{-n(L+1)(-\beta+1/L-1/(L+1)+\beta)} \\ &\leq 2^{-n(L+1)((L+1-L)/L(L+1))} \\ &\leq 2^{-n/L} \end{aligned}$$

It follows that for any  $n$ , if  $C$  is a collection of  $2^{\lfloor Rn \rfloor}$  strings of length  $n$  that we pick at random, the probability that no string  $\sigma$  of length  $n$  has a hamming distance smaller than  $\theta$  with more than  $L$  strings of  $C$ , is positive. In particular, for any  $n$ , there exists such a collection of strings.  $\square$

We can now prove that only 0, 1/2 and 1 can be realized by  $\Gamma$  values of sequences. First by [29], if  $X$  compute a function bounded by  $2^{(2^n)}$  which equals infinitely often every computable function bounded by  $2^{(2^n)}$ , then  $\Gamma(X) = 0$ : First, it is also easy to show that if  $f$  is  $2^{(2^n)}$ -i.o.e., then for any  $c$ ,  $f$  computes a function which is  $2^{(2^{c \times n})}$ -i.o.e. Second, it is easy to show that if  $f$  is  $2^{(2^{c \times n})}$ -i.o.e. then  $\gamma(f) < 1/(c + 1)$ .

**Theorem 5.6.** *Let  $1/2 < \alpha < 1$ . If  $\Gamma(X) < 1 - \alpha$  then  $X$  is  $2^{(2^n)}$ -i.o.e. and hence  $\Gamma(X) = 0$ .*

*Proof.* Suppose  $\Gamma(X) < 1 - \alpha$ . In particular from Proposition 5.4,  $X$  computes a function  $f$  which is  $2^{\lfloor 2^{n/k} \rfloor}$ -i.o. $\alpha$ -e. for some  $k \in \omega$ .

Using Theorem 5.5, we pick  $L \in \omega$  and  $0 < R < 1$  such that for any  $n$ , there exists a collection  $C_n$  of  $2^{\lfloor Rn \rfloor}$  strings of length  $n$ , such that no string  $\sigma$  of length  $n$  has a Hamming distance less than  $\theta = 1 - \alpha$  with more than  $L$  strings of  $C$ . Note that such a collection of strings  $C_n$  is computable uniformly in  $n$ . Uniformly computable in  $n$  we fix a listing  $\sigma_0^n, \sigma_1^n, \dots, \sigma_{2^{\lfloor Rn \rfloor} - 1}^n$  of the elements of  $C_n$ .

We define the following  $X$ -computable  $L$ -trace  $\{T_n\}_{n \in \omega}$ : For any  $n$ ,  $T_n$  is the collection of integer  $i$  such that the hamming distance between  $[f(n)]$  and  $\sigma_i^{\lfloor 2^{n/k} \rfloor}$  is less than  $1 - \alpha$ . Note that each  $T_n$  is  $X$ -computable uniformly

in  $n$  and that  $|T_n| \leq L$  (possibly  $T_n$  is also empty). Note also that the values of  $T_n$  are bounded by  $2^{\lfloor R2^{n/k} \rfloor}$ .

We claim that every computable function  $g < 2^{\lfloor R2^{n/k} \rfloor}$  is traced by  $T_n$ . Indeed, given such a computable function  $g$ , consider the computable function  $g'$  defined by  $g'(n) = \sigma_i^{\lfloor 2^{n/k} \rfloor}$  if  $g(n) = i$ . We have that  $g'$  is computable, and furthermore  $g'(n) \leq 2^{\lfloor 2^{n/k} \rfloor}$ . As  $f$  is  $2^{\lfloor 2^{n/k} \rfloor}$ -i.o. $\alpha$ -e., there exist infinitely many  $m$  such that  $d([f(m)], [g'(m)]) < 1 - \alpha$ . Then, by definition of  $\{T_n\}_{n \in \omega}$ , we have  $g(m) \in T_m$  for each of these  $m$ .

Thus every computable function bounded by  $2^{\lfloor R2^{n/k} \rfloor}$  is captured infinitely often by  $\{T_n\}_{n \in \omega}$ .

Now, either the trace  $T_{2n}$  must capture infinitely often every computable function bounded by  $2^{\lfloor R2^{2n/k} \rfloor}$ , or the trace  $T_{2n+1}$  must capture infinitely often every computable function bounded by  $2^{\lfloor R2^{(2n+1)/k} \rfloor}$ , as otherwise, by combining the two computable witnesses that neither is the case, we would have a computable function bounded by  $2^{\lfloor R2^{n/k} \rfloor}$  and not traced by  $\{T_n\}_{n \in \omega}$ . In either case,  $\{T_n\}_{n \in \omega}$  can compute a trace which traces every function bounded by  $2^{\lfloor R2^{2n/k} \rfloor}$  (Note that a trace capturing infinitely often every computable function bounded by  $F$ , also captures infinitely often every computable function bounded by  $G < F$ ).

By iterating this argument,  $X$  can compute an  $L$ -trace  $\{T_n\}_{n \in \omega}$  which captures infinitely often every function bounded by  $2^{L2^n}$ . We can also without loss of generality assume that each element of each  $T_n$  is bounded by  $2^{L2^n}$ , and thus coded on exactly  $L2^n$  bits. We now use the fact that  $|T_n| \leq L$  for every  $n$ , to compute using  $T_n$  a function  $h \leq 2^{2^n}$  which is equal infinitely often to every computable function bounded by  $2^{2^n}$ .

First for every  $n$ , we add if necessary some elements in  $T_n$  such that  $|T_n| = L$ . Then we view each element  $e_i$  of  $T_n$  as an  $L$ -tuple  $\langle e_i^1, \dots, e_i^L \rangle$ . Formally  $e_i^j$  is the  $j$ -th block of  $2^n$  consecutive bits. Consider  $L$  distinct  $X$ -computable functions  $h_1, \dots, h_L$  given by  $h_i(n) = e_i^i$  where  $e_i = \langle e_i^1, \dots, e_i^i, \dots, e_i^L \rangle$  is the  $i$ -th element of  $T_n$ . We claim that at least one  $h_i$  is  $2^{(2^n)}$ -i.o.e. Suppose otherwise, and consider the  $L$  computable functions  $p_1, \dots, p_L$  witnessing that. Then the computable function  $p(n) = \langle p_1(n), \dots, p_L(n) \rangle$  is never captured by  $T_n$ , as the  $i$ -th component of  $p(n)$  (seen as a  $L$ -tuple) is different from the  $i$ -th component of the  $i$ -th element of  $T_n$  (seen as a  $L$ -tuple). This contradicts our hypothesis. So at least one  $h_i$  is  $2^{(2^n)}$ -i.o.e.

Note that  $h_i$  is computable from  $X$ . As in [29, Thm. III.4] from  $h_i$  we can compute functions which are  $2^{(a^n)}$ -i.o.e. for any  $a \in \omega$ ; the binary sequence encoding each of these function have a  $\gamma$  value  $\leq 1/a$ .  $\square$

Note that all the reductions are  $tt$ . Thus this also solves the  $\Gamma$  question in the  $tt$  degrees.

## 6. BRENDLE AND NIES: ANALOG FOR CARDINAL CHARACTERISTICS OF MONIN'S SOLUTION TO THE $\Gamma$ QUESTION

For background and definitions of the characteristics see last year's blog [12, Section 7]. In analogy to Monin's post above, we will show that  $\mathfrak{d}(p) = \mathfrak{d}(\neq^*, 2^{(2^n)})$  and  $\mathfrak{b}(p) = \mathfrak{b}(\neq^*, 2^{(2^n)})$  for each  $p \in (0, 1/2)$ .

For convenience here are the main definitions:

Let  $R \subseteq X \times Y$  be a relation between spaces  $X, Y$  (such as Baire space) satisfying  $\forall x \exists y (xRy)$  and  $\forall y \exists x \neg(xRy)$ . Let  $S = \{\langle y, x \rangle \in Y \times X : \neg xRy\}$ .

**Definition 6.1.** We write

$$\mathfrak{d}(R) = \min\{|G| : G \subseteq Y \wedge \forall x \in X \exists y \in G xRy\}.$$

$$\mathfrak{b}(R) = \mathfrak{d}(S) = \min\{|F| : F \subseteq X \wedge \forall y \in Y \exists x \in F \neg xRy\}.$$

We will study  $\mathfrak{d}(R)$  and  $\mathfrak{b}(R)$  for two types of relations  $R$ .

1. Let  $h: \omega \rightarrow \omega$  (usually unbounded). Define for  $x \in {}^\omega\omega$  and  $y \in \Pi_n\{0, \dots, h(n) - 1\}$ ,

$$x \neq_h^* y \Leftrightarrow \forall^\infty n [x(n) \neq y(n)].$$

2. Let  $0 \leq p \leq 1/2$ . Define, for  $x, y \in {}^\omega 2$

$$x \sim_p y \Leftrightarrow \rho(x \leftrightarrow y) > p,$$

where  $x \leftrightarrow y$  is the set of  $n$  such that  $x(n) \neq y(n)$ , and  $\rho$  denotes the lower density:  $\rho(z) = \liminf_n |z \cap n|/n$ .

It will be helpful to express Definition 6.1 for these relations in words.

$\mathfrak{d}(\neq_h^*)$  is the least size of a set  $G$  of  $h$ -bounded functions so that for each function  $x$  there is a function  $y$  in  $G$  such that  $\forall^\infty n [x(n) \neq y(n)]$ . (Of course it suffices to require this for  $h$ -bounded  $x$ .)

$\mathfrak{b}(\neq_h^*)$  is the least size of a set  $F$  of functions such that for each  $h$ -bounded function  $y$ , there is a function  $x$  in  $F$  such that  $\exists^\infty n x(n) = y(n)$ . (Of course we can require that each function in  $F$  is  $h$ -bounded.)

$\mathfrak{d}(\sim_p)$  is the least size of a set  $G$  of bit sequences so that for each sequence  $x$  there is a sequence  $y$  in  $G$  so that  $\rho(x \leftrightarrow y) > p$ .

$\mathfrak{b}(\sim_p)$  is the least size of a set  $F$  of bit sequences such that for each bit sequence  $y$ , there is a sequence  $x$  in  $F$  such that  $\rho(x \leftrightarrow y) \leq p$ .

**Definition 6.2.** Let  $h$  be a function of the form  $2^{\hat{h}}$  with  $\hat{h}: \omega \rightarrow \omega$ , and let  $X_h$  be the space of all  $h$ -bounded functions. For such a function we view  $x(n)$  either as a number, or as a binary string of length  $\hat{h}(n)$  via the binary expansion with leading zeros allowed. We define  $L_h: X_h \rightarrow {}^\omega 2$  by  $L_h(x) = \prod_n x(n)$ , i.e. the concatenation of these strings. We let  $K_h: {}^\omega 2 \rightarrow X_h$  be the inverse of  $L_h$ .

We begin with some preliminary facts of independent interest. On occasion we denote a function  $\lambda n.f(n)$  simply by  $f(n)$ . The next lemma amplifies functions without changing the cardinal characteristics.

**Lemma 6.3.** (i) *Let  $h$  be nondecreasing and  $g(n) = h(2n)$ . We have  $\mathfrak{d}(\neq^*, h) = \mathfrak{d}(\neq^*, g)$  and  $\mathfrak{b}(\neq^*, h) = \mathfrak{b}(\neq^*, g)$ .*  
 (ii) *For each  $a, b > 1$  we have  $\mathfrak{d}(\neq^*, 2^{(a^n)}) = \mathfrak{d}(\neq^*, 2^{(b^n)})$  and  $\mathfrak{b}(\neq^*, 2^{(a^n)}) = \mathfrak{b}(\neq^*, 2^{(b^n)})$ .*

*Proof.* (i) Trivially,  $h \leq g$  implies that  $\mathfrak{d}(\neq^*, h) \geq \mathfrak{d}(\neq^*, g)$  and  $\mathfrak{b}(\neq^*, h) \leq \mathfrak{b}(\neq^*, g)$ . So it suffices to show two inequalities.

$\mathfrak{d}(\neq^*, h) \leq \mathfrak{d}(\neq^*, g)$ : Let  $G$  be a witness set for  $\mathfrak{d}(\neq^*, g)$ . Note that  $G$  is also a witness set for  $\mathfrak{d}(\neq^*, h(2n+1))$ . Let  $\widehat{G} = \{p_0 \oplus p_1 : p_0, p_1 \in G\}$ , where  $(p_0 \oplus p_1)(2m+i) = p_i(m)$  for  $i = 0, 1$ . Each function in  $\widehat{G}$  is bounded by  $h$ . Since  $G$  is infinite,  $|\widehat{G}| = |G|$ . Clearly  $\widehat{G}$  is a witness set for  $\mathfrak{d}(\neq^*, h)$ .

$\mathfrak{b}(\neq^*, h) \geq \mathfrak{b}(\neq^*, g)$ : Let  $F$  be a witness set for  $\mathfrak{b}(\neq^*, h)$ . Let  $\widehat{F}$  consist of the functions of the form  $n \rightarrow p(2n)$ , or of the form  $n \rightarrow p(2n+1)$ , where  $p \in F$ . Then  $|\widehat{F}| = |F|$ , and each function in  $\widehat{F}$  is  $g$  bounded.

Clearly,  $\widehat{F}$  is a witness set for  $\mathfrak{b}(\neq^*, g)$ : if  $q$  is  $g$ -bounded, then  $\widehat{q}$  is  $h$  bounded where  $\widehat{q}(2n+i) = q(n)$  for  $i = 0, 1$ . Let  $p \in F$  be such that  $\exists^\infty k p(k) = \widehat{q}(k)$ . Let  $i \leq 1$  be such that infinitely many such  $k$  have parity  $i$ . Then the function  $n \rightarrow p(2n+i)$  which is in  $\widehat{F}$  is as required.

(ii) is immediate from (i) by iteration using that  $a^{2^i} > b$  and  $b^{2^i} > a$  for sufficiently large  $i$ .  $\square$

**Lemma 6.4.** *Let  $a \in \omega - \{0\}$ . We have  $\mathfrak{d}(\neq^*, 2^{(a^n)}) \leq \mathfrak{d}(1/a)$  and  $\mathfrak{b}(\neq^*, 2^{(a^n)}) \geq \mathfrak{b}(1/a)$ .*

*Proof.* Let  $I_m$  for  $m \geq 2$  be the  $m-1$ -th consecutive interval of length  $a^m$  in  $\omega - \{0\}$ , i.e.

$$I_m = \left[ \frac{a^m - 1}{a - 1}, \frac{a^{m+1} - 1}{a - 1} \right).$$

First let  $G$  be a witness set for  $\mathfrak{d}(1/a)$ . Let  $h(n) = 2^{(a^n)}$ . We show that  $\widehat{G} = \{K_h(y) : y \in G\}$  is a witness set for  $\mathfrak{d}(\neq^*, 2^{(a^n)})$ . Otherwise there is a sequence  $z \in {}^\omega 2$  such that for each  $x \in {}^\omega \omega$  there are infinitely many  $m$  with  $x(m) = K_h(z)(m)$ . Let  $y'$  be the complement  $\omega - z$  of  $z$ , that is 0s and 1s are interchanged. Then for infinitely many  $m$ ,  $L_h(x)(i) \neq y'(i)$  for each  $i \in I_m$ . If we let  $n = 1 + \max I_m$ , the proportion of  $i < n$  such that  $L_h(x)(i) = y'(i)$  is therefore at most  $(a^m - 1)/(a^{m+1} - 1)$ , which converges to  $1/a$  as  $m \rightarrow \infty$ . This contradicts the choice of  $G$ .

Now let  $F$  be a witness set for  $\mathfrak{b}(\neq^*, h)$ . Let  $\widehat{F} = \{\omega - L_h(x) : x \in F\}$ . For each  $y \in 2^\mathbb{N}$  there is  $x \in F$  such that  $\exists^\infty n K_h(y)(n) = x(n)$ . This implies  $\rho(y \leftrightarrow x') \leq 1/a$  where  $x' = \omega - L_h(x) \in \widehat{F}$ . Hence  $\widehat{F}$  is a witness set for  $\mathfrak{b}(1/a)$ .  $\square$

**Theorem 6.5.** *Fix any  $p \in (0, 1/2)$ . We have  $\mathfrak{d}(p) = \mathfrak{d}(\neq^*, 2^{(2^n)})$  and  $\mathfrak{b}(p) = \mathfrak{b}(\neq^*, 2^{(2^n)})$ .*

*Proof.* By the two foregoing lemmas we have  $\mathfrak{d}(p) \geq \mathfrak{d}(\neq^*, 2^{(2^n)})$  and  $\mathfrak{b}(p) \leq \mathfrak{b}(\neq^*, 2^{(2^n)})$ . It remains to show the converse inequalities:  
 $\mathfrak{d}(p) \leq \mathfrak{d}(\neq^*, 2^{(2^n)})$  and  $\mathfrak{b}(p) \geq \mathfrak{b}(\neq^*, 2^{(2^n)})$ .

**Definition 6.6.** For strings  $x, y$  of length  $r$ , the normalised Hamming distance is defined as the proportion of bits on which  $x, y$  disagree, that is,

$$d(x, y) = \frac{1}{r} |\{i: x(n)(i) \neq y(n)(i)\}|$$

**Definition 6.7.** Let  $h$  be a function of the form  $2^{\hat{h}}$  with  $\hat{h}: \omega \rightarrow \omega$ , and let  $X = Y = X_h$  be the space of  $h$ -bounded functions. Let  $q \in (0, 1/2)$ . We define a relation on  $X \times Y$  by

$$x \neq_{\hat{h}, q}^* y \Leftrightarrow \forall^\infty n [d(x(n), y(n)) \geq q]$$

namely for a.e.  $n$  the strings  $x(n)$  and  $y(n)$  disagree on a proportion of at least  $q$  of the bits. We will usually write  $\langle \neq^*, \hat{h}, q \rangle$  for this relation.

**Claim 6.8.** For each  $c \in \omega$  there is  $k \in \omega$  such that

$$\begin{aligned} \mathfrak{d}(q - 2/c) &\leq \mathfrak{d}(\neq^*, \lfloor 2^{n/k} \rfloor, q), \text{ and} \\ \mathfrak{b}(q - 2/c) &\geq \mathfrak{b}(\neq^*, \lfloor 2^{n/k} \rfloor, q). \end{aligned}$$

To see this, let  $k$  be large enough so that  $2^{1/k} - 1 < \frac{1}{2c}$ . Let  $\hat{h}(n) = \lfloor 2^{n/k} \rfloor$  and  $h = 2^{\hat{h}}$ . Write  $H(n) = \sum_{r \leq n} \hat{h}(r)$ . Given an infinite bit sequence, we refer to the bits with position in an interval  $[H(n), H(n+1))$  as *Block  $n$*  (the first block is Block 0). By Monin's 2016 logic blog entry, for sufficiently large  $n$ ,

$$\hat{h}(n+1) \leq \frac{1}{c} H(n).$$

For the inequality involving  $\mathfrak{d}$ , let  $G$  be a witness set for  $\mathfrak{d}(\neq^*, \hat{h}, q)$ . Thus, for each function  $x < h$  there is a function  $y \in G$  such that for almost all  $n$ ,  $L_h(x), L_h(y)$  disagree on a proportion of  $q$  bits of Block  $n$ . Let  $z$  be the complement of  $L_h(y)$ . Given  $m$ , let  $n$  be such that  $H(n) \leq m < H(n+1)$ . Since  $m - H(n) \leq \frac{1}{c} H(n)$ , for large enough  $m$ ,  $L_h(x)$  and  $z$  agree up to  $m$  on a proportion of at least  $q - 1.5/c$  bits. So the set of complements of the  $L_h(y)$ ,  $y \in G$ , forms a witness set for  $\mathfrak{d}(q - 2/c)$  as required.

For the inequality involving  $\mathfrak{b}$ , let  $F$  be a witness set for  $\mathfrak{b}(q - 2/c)$ . Thus, for each  $y \in 2^{\mathbb{N}}$  there is  $x \in F$  such that  $\rho(y \leftrightarrow x) \leq q - 2/c$ . Let  $\hat{F} = \{K_h(1 - x): x \in F\}$ . We show that  $\hat{F}$  is a witness set for  $\mathfrak{b}(\neq^*, \lfloor 2^{n/k} \rfloor, q)$ .

Give a function  $y < h$ , let  $y' = L_h(y)$ . There is  $x \in F$  such that  $\rho(y' \leftrightarrow x) \leq q - 2/c$ , and hence  $\bar{\rho}(y' \leftrightarrow x') \geq 1 - q + 2/c$  where  $x' = 1 - x$  is the complement and  $\bar{\rho}$  denotes the upper density. Then there are infinitely many  $m$  such that the strings  $y' \upharpoonright_m$  and  $x' \upharpoonright_m$  agree on a proportion of  $> q + 1/c$  bits. Suppose that  $H(n) \leq m < H(n+1)$  then the contribution of disagreement of Block  $n$  is at most  $1/c$ . So there are infinitely many  $k$  so that in Block  $k$ ,  $y'$  and  $x'$  agree on a proportion of more than  $1 - q$  bits, and hence disagree on a proportion of fewer than  $q$  bits. This shows the claim.

As in Monin's entry we use the list decoding capacity theorem from the theory of error-correcting codes. Given  $q$  as above and  $L \in \omega$ , for each  $r$



there is a “fairly large” set  $C$  of strings of length  $r$  (the allowed code words) such that for each string, at most  $L$  strings in  $C$  have normalised Hamming distance less than  $q$  from  $\sigma$ . (Hence there is only a small set of strings that could be the error-corrected version of  $\sigma$ .) Given string  $\sigma$  of length  $r$ , let  $B_q(\sigma)$  denote an open ball around  $\sigma$  in the normalised Hamming distance, namely,  $B_q(\sigma) = \{\tau \in {}^r 2 : \sigma, \tau \text{ disagree on fewer than } qr \text{ bits}\}$

**Lemma 6.9** (List decoding). *Let  $q \in (0, 1/2)$ . There are  $\epsilon > 0$  and  $L \in \omega$  such that for each  $r$ , there is a set  $C$  of  $2^{\lfloor \epsilon r \rfloor}$  strings of length  $r$  as follows:*

$$\forall \sigma \in {}^r 2 [ |B_q(\sigma) \cap C| \leq L ].$$

For  $L \in \omega$ , an  $L$ -slalom is a function  $s: \omega \rightarrow \omega^{[\leq L]}$ , i.e. a function that maps natural numbers to sets of natural numbers with a size of at most  $L$ .

**Definition 6.10.** Fix a function  $u: \omega \rightarrow \omega$  and  $L \in \omega$ . Let  $X$  be the space of  $L$ -slaloms  $s$  such that  $\max s(n) < u(n)$  for each  $n$ , and let  $Y$  be the set of functions such that  $y(n) < u(n)$  for each  $n$ . Define a relation on  $X \times Y$  by

$$s \not\preceq_{u,L}^* y \Leftrightarrow \forall^\infty n [s(n) \not\preceq y(n)].$$

We will write  $\langle \not\preceq^*, u, L \rangle$  for this relation.

**Claim 6.11.** *Given  $q < 1/2$ , let  $L, \epsilon$  be as in Lemma 6.9. Fix a nondecreasing function  $\hat{h}$ , and let  $u(n) = 2^{\lfloor \epsilon \hat{h}(n) \rfloor}$ . We have*

$$\mathfrak{d}(\not\preceq^*, \hat{h}, q) \leq \mathfrak{d}(\not\preceq^*, u, L) \text{ and } \mathfrak{b}(\not\preceq^*, \hat{h}, q) \geq \mathfrak{b}(\not\preceq^*, u, L).$$

For the inequality involving  $\mathfrak{d}$ , let  $G$  be a set of functions bounded by  $u$  such that  $|G| < \mathfrak{d}(\not\preceq^*, \hat{h}, q)$ . We show that  $G$  is not a witness set for the right hand side  $\mathfrak{d}(\not\preceq^*, u, L)$ .

For each  $r$  of the form  $\hat{h}(n)$  choose a set  $C = C_r$  as in Lemma 6.9. Since  $|C_r| = 2^{\lfloor \epsilon r \rfloor}$  we may choose a sequence  $\langle \sigma_i^r \rangle_{i < 2^{\lfloor \epsilon r \rfloor}}$  listing  $C_r$  without repetitions. For a function  $y < u$  let  $\tilde{y}$  be the function given by  $\tilde{y}(n) = \sigma_{y(n)}^{\hat{h}(n)}$ . Thus  $\tilde{y}(n)$  is a binary string of length  $\hat{h}(n)$ . Let  $\tilde{G} = \{\tilde{y} : y \in G\}$ . Then  $|\tilde{G}| = |G| < \mathfrak{d}(\not\preceq^*, \hat{h}, q)$ . So there is a function  $x$  with  $x(n) \in \hat{h}(n)2$  for each  $n$  such that for each  $y \in \tilde{G}$  we have  $\exists^\infty n [d(x(n), y(n)) < q]$ . Let  $s$  be the slalom given by

$$s(n) = \{i : d(x(n), \sigma_i^{\hat{h}(n)}) < q\}.$$

Note that by the choice of the  $C_r$  according to Lemma 6.9,  $s$  is an  $L$ -slalom. By the definitions, for each  $y \in G$  we have  $\exists^\infty n [s(n) \ni y(n)]$ . So  $G$  is not a witness set for  $\mathfrak{d}(\not\preceq^*, u, L)$ .

For the inequality involving  $\mathfrak{b}$ , suppose  $F$  is a witness set for  $\mathfrak{b}(\not\preceq^*, \hat{h}, q)$ . That is, for each  $h = 2^{\hat{h}}$ -bounded function  $y$ , there is  $x \in F$  such that

$$\exists^\infty n [d(x(n), y(n)) < q]$$

(as usual we view  $x(n), y(n)$  as binary strings of length  $\hat{h}(n)$ ). For  $x \in F$  let  $s_x$  be the  $L$ -slalom such that

$$s_x(n) = \{i < u(n) : d(\sigma_i^{\hat{h}(n)}, x(n)) < q\}.$$

Let  $\widehat{F} = \{s_x : x \in F\}$ . Given an  $u$ -bounded function  $y$ , let  $y'(n) = \sigma_{y(n)}^{\widehat{h}(n)}$ . There is  $x \in F$  such that  $d(x(n), y'(n)) < q$  for infinitely many  $n$ . This means that  $y(n) \in s_x(n)$ . Hence  $\widehat{F}$  is a witness set for  $\mathfrak{b}(\not\exists^*, u, L)$ . This shows the claim.

We next need an amplification tool in the context of slaloms. The proof is almost verbatim the one in Lemma 6.3(i), so we omit it.

**Claim 6.12.** *Let  $L \in \omega$ , let the function  $u$  be nondecreasing and let  $w(n) = u(2n)$ . We have  $\mathfrak{d}(\not\exists^*, u, L) = \mathfrak{d}(\not\exists^*, w, L)$  and  $\mathfrak{b}(\not\exists^*, u, L) = \mathfrak{b}(\not\exists^*, w, L)$ .*

Iterating the claim, starting with the function  $\widehat{h}(n) = \lfloor 2^{n/k} \rfloor$  with  $k$  as in Claim 22.5, we obtain that  $\mathfrak{d}(\not\exists^*, 2^{\widehat{h}}, L) = \mathfrak{d}(\not\exists^*, 2^{(L^{2^n})}, L)$ , and similarly for  $\mathfrak{b}$ . It remains to verify the following.

**Claim 6.13.**  $\mathfrak{d}(\not\exists^*, 2^{(L^{2^n})}, L) \leq \mathfrak{d}(\not\exists^*, 2^{(2^n)})$  and  $\mathfrak{b}(\not\exists^*, 2^{(L^{2^n})}, L) \geq \mathfrak{b}(\not\exists^*, 2^{(2^n)})$ .

Given  $n$ , we write a number  $k < 2^{(L^{2^n})}$  in binary with leading zeros if necessary, and so can view  $k$  as a binary string of length  $L^{2^n}$ . We view such a string as consisting of  $L$  consecutive blocks of length  $2^n$ .

For the inequality involving  $\mathfrak{d}$ , let  $G$  be a witness set for  $\mathfrak{d}(\not\exists^*, 2^{(2^n)})$ . For functions  $y_1, \dots, y_L$  such that  $y_i(n) < 2^{(2^n)}$  for each  $n$ , let  $(y_1, \dots, y_L)$  denote the function  $y$  with  $y(n) < 2^{(L^{2^n})}$  for each  $n$  such that the  $i$ -th block of  $y(n)$  equals  $y_i(n)$  for each  $i$  with  $1 \leq i \leq L$ . Let

$$\widehat{G} = \{(y_1, \dots, y_n) : y_1, \dots, y_L \in G\}.$$

Since  $G$  is infinite we have  $|\widehat{G}| = |G|$ . We check that  $\widehat{G}$  is a witness set for the left hand side  $\mathfrak{d}(\not\exists^*, 2^{(L^{2^n})})$ . Given an  $L$ -slalom  $s$  bounded by  $2^{(L^{2^n})}$  we may assume that  $s(n)$  has exactly  $L$  members, and they are binary strings of length  $L^{2^n}$ . For  $i \leq L$  let  $x_i(n)$  be the  $i$ -th block of the  $i$ -th string in  $s(n)$ , so that  $|x_i(n)| = 2^n$ . Viewing the  $x_i$  as functions bounded by  $2^{(2^n)}$ , we can choose  $y_1, \dots, y_L \in G$  such that  $\forall^\infty n x_i(n) \neq y_i(n)$ . Let  $y = (y_1, \dots, y_n) \in \widehat{G}$ . Then  $\forall^\infty n [s(n) \ni y(n)]$ , as required.

For the inequality involving  $\mathfrak{b}$  let  $F$  be a witness set for  $\mathfrak{b}(\not\exists^*, 2^{(L^{2^n})})$ . That is,  $F$  is a set of  $L$ -slaloms  $s$  such that for each function  $y$  with  $y(n) < 2^{(L^{2^n})}$ , there is  $s \in F$  such that  $s(n) \ni y(n)$  for infinitely many  $n$ .

Let  $\widehat{F}$  be the set of functions  $s_i$ , for  $s \in F$  and  $i < L$ , such that  $s_i(n)$  is the  $i$ -th block of the  $i$ -th element of  $s(n)$  (as before we may assume that each string in  $s(n)$  has length  $L^{2^n}$ ). Now let  $y$  be a given function bounded by  $2^{(2^n)}$ . Let  $y'$  be the function bounded by  $2^{(L^{2^n})}$  such that for each  $n$ , each block of  $y'(n)$  equals  $y(n)$ . There is  $s \in F$  such that  $s(n) \ni y'(n)$  for infinitely many  $n$ . There is  $i < L$  such that  $y'(n)$  is the  $i$ -th string in  $s(n)$  for infinitely many of these  $n$ , and hence  $y(n) = s_i(n)$ . Thus  $\widehat{F}$  is a witness set for  $\mathfrak{b}(\not\exists^*, 2^{(2^n)})$ . This proves the claim.

We can now summarise the argument that  $\mathfrak{d}(p) \leq \mathfrak{d}(\not\exists^*, 2^{(2^n)})$ . Pick  $c$  large enough such that  $q = p + 2/c < 1/2$ .

By Claim 22.5 there is  $k$  such that

$$\mathfrak{d}(p) \leq \mathfrak{d}(\not\exists^*, \lfloor 2^{n/k} \rfloor, q).$$

By Claim 6.11 there are  $L, \epsilon$  such that where  $\widehat{h}(n) = \lfloor 2^{n/k} \rfloor$ , we have

$$\mathfrak{d}(\neq^*, \widehat{h}, q) \leq \mathfrak{d}(\neq^*, u, L),$$

where  $u(n) = 2^{\lfloor \epsilon \widehat{h}(n) \rfloor}$ .

Applying Claim 6.12 sufficiently many times we have

$$\mathfrak{d}(\neq^*, u, L) \leq \mathfrak{d}(\neq^*, 2^{(L^{2^n})}, L).$$

Finally,  $\mathfrak{d}(\neq^*, 2^{(L^{2^n})}, L) \leq \mathfrak{d}(\neq^*, 2^{(2^n)})$  by Claim 6.13. The argument for  $\mathfrak{b}(p) \geq \mathfrak{b}(\neq^*, 2^{(2^n)})$  is the exact dual.  $\square$

## 7. NIES: ANSWERING THE $\Delta$ QUESTION

We use the notation in [5]. Let  $R \subseteq X \times Y$  be a relation between spaces  $X, Y$ , and let  $S = \{\langle y, x \rangle \in Y \times X : \neg xRy\}$ . Suppose we have specified what it means for objects  $x$  in  $X$ ,  $y$  in  $Y$  to be computable in a Turing oracle  $A$ . We denote this by for example  $x \leq_T A$ . In particular, for  $A = \emptyset$  we have a notion of computable objects.

Let the variable  $x$  range over  $X$ , and let  $y$  range over  $Y$ . We define the highness properties

$$\mathcal{B}(R) = \{A : \exists y \leq_T A \forall x \text{ computable } [xRy]\}$$

$$\mathcal{D}(R) = \mathcal{B}(S) = \{A : \exists x \leq_T A \forall y \text{ computable } [\neg xRy]\}$$

1. Let  $h: \omega \rightarrow \omega - \{0, 1\}$ . Define for  $x \in {}^\omega\omega$  and  $y \in \prod_n \{0, \dots, h(n) - 1\} \subseteq {}^\omega\omega$ ,

$$x \neq_h^* y \Leftrightarrow \forall^\infty n [x(n) \neq y(n)].$$

2. Let  $0 \leq p \leq 1/2$ . Define, for  $x, y \in {}^\omega 2$

$$x \sim_p y \Leftrightarrow \underline{\rho}(x \leftrightarrow y) > p,$$

where  $x \leftrightarrow y$  is the set of  $n$  such that  $x(n) = y(n)$ , and  $\underline{\rho}$  denotes the lower density:  $\underline{\rho}(z) = \liminf_n |z \cap n|/n$ .

It may be helpful to separately state two special cases.

**Definition 7.1.** For a computable function  $h$ , we let  $\mathcal{B}(\neq_h^*)$  denote the class of oracles  $A$  that compute a function  $y < h$  such that for each computable function  $x$ , we have  $\forall^\infty n [x(n) \neq y(n)]$ .

For  $p < 1/2$ , we let  $\mathcal{B}(\sim_p)$ , or  $\mathcal{B}(p)$  for short, denote the class of oracles  $A$  that compute a set  $y$  such that for each computable set  $x$ , we have  $\underline{\rho}(x \leftrightarrow y) > p$ .

Recall Definition 4.1 and that for each  $p$  with  $0 \leq p < 1/2$ ,

$$\Delta(A) > p \Rightarrow A \in \mathcal{B}(\sim_p) \Rightarrow \Delta(A) \geq p.$$

We show that  $\mathcal{B}(\sim_p) = \mathcal{B}(\neq^*, 2^{(2^n)})$  for each  $p \in (0, 1/2)$ . In particular,  $\Delta(A) > 0 \Rightarrow \Delta(A) = 1/2$  so there are only two possible  $\Delta$  values.

We begin with some preliminary facts of independent interest. On occasion we denote a function  $\lambda n.f(n)$  simply by  $f(n)$ .

**Lemma 7.2.** (i) Let  $h$  be nondecreasing and  $g(n) = h(2n)$ . We have  $\mathcal{B}(\neq^*, h) = \mathcal{B}(\neq^*, g)$ .

(ii) For each  $a, b > 1$  we have  $\mathcal{B}(\neq^*, 2^{(a^n)}) = \mathcal{B}(\neq^*, 2^{(b^n)})$ .

*Proof.* (i) Trivially,  $h \leq g$  implies that  $\mathcal{B}(\neq^*, h) \subseteq \mathcal{B}(\neq^*, g)$ . So it suffices to show the converse inclusion  $\mathcal{B}(\neq^*, h) \supseteq \mathcal{B}(\neq^*, g)$ .

Let  $y \leq_T A$ ,  $y < g$  be a function witnessing that  $A \in \mathcal{B}(\neq^*, g)$ . Let  $\hat{y}(2n+i) = y(n)$  for  $i \leq 1$ , so that  $\hat{y} < h$ . Given any computable function  $x$ , for almost every  $n$  we have  $x(2n) \neq y(n)$  and  $x(2n+1) \neq y(n)$ . Therefore  $\forall^\infty n [x(n) \neq \hat{y}(n)]$ . Hence  $\hat{y}$  is a witness for  $A \in \mathcal{B}(\neq^*, h)$ .

(ii) is immediate from (i) by iteration using that  $a^{2^i} > b$  and  $b^{2^i} > a$  for sufficiently large  $i$ .  $\square$

Recall Def. 6.2 of the  $L_h$  and  $K_h$  operators.

**Lemma 7.3.** Let  $a \in \omega - \{0\}$ . We have  $\mathcal{B}(\neq^*, 2^{(a^n)}) \supseteq \mathcal{B}(1/a)$ .

*Proof.* Let  $I_m$  for  $m \geq 2$  be the  $m-1$ -th consecutive interval of length  $a^m$  in  $\omega - \{0\}$ , i.e.

$$I_m = \left[ \frac{a^m - 1}{a - 1}, \frac{a^{m+1} - 1}{a - 1} \right).$$

Let  $h(m) = 2^{a^m}$ . Let  $y \leq_T A$  witness that  $A \in \mathcal{B}(1/a)$ , and let  $\hat{y} = K_h(y)$ . Given a computable function  $x < h$ , let  $x' = 1 - L_h(x)$ . Since  $\rho(x' \leftrightarrow y) > 1/a$ , for large enough  $n$ , there is  $k \in I_n$  such that  $x'(i) = y(i)$ . Hence we cannot have  $x(n) = \hat{y}(n)$ . Thus  $\hat{y}$  witnesses that  $A \in \mathcal{B}(\neq^*, 2^{(a^n)})$ .  $\square$

A similar argument shows that  $\mathcal{B}(\neq^*, 2^{\hat{h}(m)}) \supseteq \mathcal{B}(0)$  for any computable function  $\hat{h}$  such that  $\forall a \forall^\infty m \hat{h}(m) \geq a^m$ . Now the  $m$ -th interval has length  $\hat{h}(m)$ .

**Theorem 7.4.** Fix any  $p \in (0, 1/2)$ . We have  $\mathcal{B}(p) = \mathcal{B}(\neq^*, 2^{(2^n)})$ .

*Proof.* The two foregoing lemmas imply  $\mathcal{B}(p) \subseteq \mathcal{B}(\neq^*, 2^{(2^n)})$ . It remains to show the converse inclusion  $\mathcal{B}(p) \supseteq \mathcal{B}(\neq^*, 2^{(2^n)})$ .

**Definition 7.5.** For strings  $x, y$  of length  $r$ , the normalised Hamming distance is defined as the proportion of bits on which  $x, y$  disagree, that is,

$$d(x, y) = \frac{1}{r} |\{i : x(n)(i) \neq y(n)(i)\}|$$

**Definition 7.6.** Let  $h$  be a function of the form  $2^{\hat{h}}$  with  $\hat{h} : \omega \rightarrow \omega$ , and let  $X = Y = X_h$  be the space of  $h$ -bounded functions. Let  $q \in (0, 1/2)$ . We define a relation on  $X \times Y$  by

$$x \neq_{h,q}^* y \Leftrightarrow \forall^\infty n [d(x(n), y(n)) \geq q]$$

namely for a.e.  $n$  the strings  $x(n)$  and  $y(n)$  disagree on a proportion of at least  $q$  of the bits. We will usually write  $\langle \neq^*, \hat{h}, q \rangle$  for this relation.

The first step makes the crucial transition from the density setting to the combinatorial setting.

**Claim 7.7.** Let  $q \in (0, 1/2)$ . For each  $c \in \omega$  such that  $2/c < q$ , there is  $k \in \omega$  such that

$$\mathcal{B}(q - 2/c) \supseteq \mathcal{B}(\neq^*, \lfloor 2^{n/k} \rfloor, q).$$

To see this, let  $k$  be large enough so that  $2^{1/k} - 1 < \frac{1}{2c}$ . Let  $\hat{h}(n) = \lfloor 2^{n/k} \rfloor$  and  $h = 2^{\hat{h}}$ . Write  $H(n) = \sum_{r \leq n} \hat{h}(r)$ . Given an infinite bit sequence, we refer to the bits with position in an interval  $[H(n), H(n+1))$  as *Block  $n$*  (the first block is Block 0). By Monin's 2016 logic blog entry, for sufficiently large  $n$ ,

$$\hat{h}(n+1) \leq \frac{1}{c} H(n).$$

Let  $y \leq_T A$  be a witness for  $A \in \mathcal{B}(\neq^*, \lfloor 2^{n/k} \rfloor, q)$ . Thus,  $y < h$  and  $\forall^\infty n [d(L_h(x)(n), L_h(y)(n)) \geq q]$ . Let  $y' = 1 - L_h(y)$ . Then

$$\forall^\infty n [d(x'(n), y'(n)) < q]$$

for each computable  $x' \in 2^\mathbb{N}$ . Suppose that  $H(n) \leq m < H(n+1)$ . Then the contribution of Block  $n$  to the proportion of disagreement between  $x', y'$  is at most  $1/c$ . So  $\rho(y' \leftrightarrow x') > q - 2/c$ . Hence  $y' \leq_T A$  is a witness for  $A \in \mathcal{B}(q - 2/c)$ . This shows the claim.

For  $L \in \omega$ , an  $L$ -slalom is a function  $s: \omega \rightarrow \omega^{[\leq L]}$ , i.e. a function that maps natural numbers to sets of natural numbers with a size of at most  $L$ .

**Definition 7.8.** Fix a function  $u: \omega \rightarrow \omega$  and  $L \in \omega$ . Let  $X$  be the space of  $L$ -slaloms (or traces)  $s$  such that  $\max s(n) < u(n)$  for each  $n$ . Thus  $s$  maps natural numbers to sets of natural numbers of size at most  $L$ , represented by strong indices. Let  $Y$  be the set of functions such that  $y(n) < u(n)$  for each  $n$ . Define a relation on  $X \times Y$  by

$$s \not\equiv_{u,L}^* y \Leftrightarrow \forall^\infty n [s(n) \not\equiv y(n)].$$

We will write  $\langle \not\equiv^*, u, L \rangle$  for this relation.

**Claim 7.9.** Given  $q < 1/2$ , let  $L, \epsilon$  be as in Lemma 6.9. Fix a nondecreasing computable function  $\hat{h}$ , and let  $u(n) = 2^{\lfloor \epsilon \hat{h}(n) \rfloor}$ . We have

$$\mathcal{B}(\neq^*, \hat{h}, q) \supseteq \mathcal{B}(\not\equiv^*, u, L).$$

For each  $r$  of the form  $\hat{h}(n)$  compute a set  $C = C_r$  as in Lemma 6.9. Since  $|C_r| = 2^{\lfloor \epsilon r \rfloor}$  there is a uniformly computable sequence  $\langle \sigma_i^r \rangle_{i < 2^{\lfloor \epsilon r \rfloor}}$  listing  $C_r$  in increasing lexicographical order.

Suppose that  $y \leq_T A$  is a witness for  $A \in \mathcal{B}(\not\equiv^*, u, L)$ . Let  $\tilde{y} < h$  be the function given by  $\tilde{y}(n) = \sigma_{y(n)}^{\hat{h}(n)}$ . We show that  $\tilde{y}$  is a witness for  $A \in \mathcal{B}(\neq^*, \hat{h}, q)$ .

For a computable function  $x < h$ , let  $s_x$  be the computable  $L$ -trace such that

$$s_x(n) = \{i < u(n) : d(\sigma_i^{\hat{h}(n)}, x(n)) < q\}.$$

Since  $y$  is a witness for  $A \in \mathcal{B}(\not\equiv^*, u, L)$ , for almost every  $n$  we have  $y(n) \notin s_x(n)$ . Hence  $d(\tilde{y}(n), x(n)) \geq q$ , as required.

We next need an amplification tool in the context of traces. The proof is almost verbatim the one in Lemma 7.2(i), so we omit it.

**Claim 7.10.** *Let  $L \in \omega$ , let the computable function  $u$  be nondecreasing and let  $w(n) = u(2n)$ . We have  $\mathcal{B}(\langle \not\exists^*, u, L \rangle) = \mathcal{B}(\langle \not\exists^*, w, L \rangle)$ .*

Iterating the claim, starting with the function  $\hat{h}(n) = \lfloor 2^{n/k} \rfloor$  with  $k$  as in Claim 7.7, we obtain that  $\mathcal{B}(\langle \not\exists^*, 2^{\hat{h}}, L \rangle) = \mathcal{B}(\langle \not\exists^*, 2^{(L2^n)}, L \rangle)$ . It remains to verify the following, which would work for any computable function  $\hat{h}(n)$  in place of the  $2^n$  in the exponents.

**Claim 7.11.**  $\mathcal{B}(\langle \not\exists^*, 2^{(L2^n)}, L \rangle) \supseteq \mathcal{B}(\langle \neq^*, 2^{(2^n)} \rangle)$ .

Given  $n$ , we write a number  $k < 2^{(L2^n)}$  in binary with leading zeros if necessary, and so can view  $k$  as a binary string of length  $L2^n$ . We view such a string as consisting of  $L$  consecutive blocks of length  $2^n$ .

Let  $y$  be a witness function for  $\mathcal{B}(\langle \neq^*, 2^{(2^n)} \rangle)$ . That is,  $y < 2^{(2^n)}$  and  $\forall^\infty n x(n) \neq y(n)$  for each computable function  $x$ . Let  $y'$  be the function bounded by  $2^{(L2^n)}$  such that for each  $n$ , each block of  $y'(n)$  equals  $y(n)$ . Given a computable  $L$ -trace  $s$  with  $\max s(n) < 2^{(L2^n)}$ , for  $i < L$  let  $x_i$  be the computable function such that  $x_i(n)$  is the  $i$ -th block of the  $i$ -th element of  $s(n)$  (as before we may assume that each string in  $s(n)$  has length  $L2^n$ ). For sufficiently large  $n$ , we have  $\forall i < L y(n) \neq x_i(n)$ . Hence  $\forall^\infty n s(n) \not\equiv y'(n)$  and  $y'$  is a witness for  $A \in \mathcal{B}(\langle \not\exists^*, 2^{(L2^n)} \rangle)$ .

We can now summarise the argument that  $\mathcal{B}(p) \supseteq \mathcal{B}(\langle \neq^*, 2^{(2^n)} \rangle)$ . Pick  $c$  large enough such that  $q = p + 2/c < 1/2$ .

By Claim 7.7 there is  $k$  such that

$$\mathcal{B}(p) \supseteq \mathcal{B}(\langle \neq^*, \lfloor 2^{n/k} \rfloor, q \rangle).$$

By Claim 7.9 there are  $L, \epsilon$  such that where  $\hat{h}(n) = \lfloor 2^{n/k} \rfloor$  and  $u(n) = 2^{\lfloor \epsilon \hat{h}(n) \rfloor}$ , we have

$$\mathcal{B}(\langle \neq^*, \hat{h}, q \rangle) \supseteq \mathcal{B}(\langle \not\exists^*, u, L \rangle).$$

Applying Claim 7.10 sufficiently many times we have

$$\mathcal{B}(\langle \not\exists^*, u, L \rangle) \supseteq \mathcal{B}(\langle \not\exists^*, 2^{(L2^n)}, L \rangle).$$

Finally,  $\mathcal{B}(\langle \not\exists^*, 2^{(L2^n)}, L \rangle) \supseteq \mathcal{B}(\langle \neq^*, 2^{(2^n)} \rangle)$  by Claim 7.11.  $\square$

We note that by the proofs, both inclusions in Theorem 7.4 are uniform in a strong sense: from a witness  $y \leq_T A$  for one property one can compute a witness  $y'$  for the other property.

As a corollary to Theorem 7.4 we obtain a proof of Proposition 4.2. If  $A$  is 2-generic then  $A$  is neither high nor d.n.c., so  $A$  is not in  $\mathcal{B}(\langle \neq^* \rangle) =$  high or d.n.c. the class where no bound is imposed on the witness function  $A$  computes. So  $A$  is not in  $\mathcal{B}(\langle \neq^*, 2^{(2^n)} \rangle)$ , hence  $\Delta(A) = 0$ .

## Part 4. Reverse mathematics

### 8. BELANGER, NIES AND SHAFER: THE STRENGTH OF RANDOMNESS EXISTENCE AXIOMS

David Belanger, André Nies and Paul Shafer others discussed the strength of randomness existence axioms at NUS and University of Ghent in February/March.

In [11, Section. 9], for a randomness notion  $\mathcal{C}$ , we defined  $\mathcal{C}_0$  to be the system  $\text{RCA} + \forall X \exists Y Y \in \mathcal{C}^X$ . For instance,  $\text{MLR}_0$  is equivalent to weak weak König's Lemma over  $\text{RCA}$ .

The system  $\text{CR}_0$  (computable randomness) appears to be equivalent to the seemingly weaker  $\text{SR}_0$  (Schnorr randomness) ([11, Prop. 9.2]; the strength of induction axioms that are needed to show this remains to be checked carefully).

**2-randomness versus weak 2-randomness.** On the other hand  $2\text{R}_0$  (the system for 2-randomness) is strictly stronger than  $\text{W2R}_0$  (the system for weak 2 randomness). To see this, take a weakly 2-random  $Z$  that does not compute a 2-random. For instance, any 2-random has hyperimmune degree. Any computably dominated ML-random  $Z$  is weakly 2-random and hence does not compute a 2-random. For each  $n$  let  $Z_n$  be the  $n$ -th column of  $Z$ , that is,  $Z_n = \{k: \langle k, n \rangle \in Z\}$ . Let  $\mathcal{M} = (\mathbb{N}, \mathcal{S})$  where  $\mathcal{S}$  consists of all the sets Turing below the join of finitely many columns of  $Z$ . Note that  $Z_n$  is weakly 2-random in any finite sum of columns not containing  $Z_n$ . So  $\mathcal{M}$  is a model of  $\text{W2R}_0$ .

We can also separate the two randomness existence axioms via an interesting mathematical consequence: Csima and Mileti [8] have shown that  $2\text{R}_0$  implies the Rainey Rambo's theorem.

**Proposition 8.1.**  *$\text{W2R}_0$  does not imply the Rainbow Ramsey's theorem.*

*Proof.* Joseph Miller has shown that the Rainbow Ramsey's theorem is equivalent over  $\text{RCA}_0$  plus some induction to the existence of a d.n.c. function relative to  $\emptyset'$ . (Detail needed here on the construction for the forward direction: recursive in a homogeneous set we obtain the function.) By [31, Exercise 4.3.18] there is a weakly 2-random set  $Z$  that does not compute a 2-fixed point free function, and hence it computes no d.n.c. function relative to  $\emptyset'$ . Construct the model  $\mathcal{M} \models \text{W2R}_0$  from  $Z$  as above. Then Rainbow Ramsey's theorem fails in  $\mathcal{M}$ .  $\square$

**Weak Demuth randomness versus WKL.**

**Definition 8.2.** A  $\Delta_2^0$  function  $f$  is  $\omega$ -c.e. if there is a computable function  $h$  such that  $h(n)$  bounds the number of changes in a computable approximation to  $f(n)$ .

A *Demuth test* is an effective sequence  $\langle \mathcal{U}_n \rangle$  of effectively open ( $\Sigma_1^0$ ) subsets of Cantor space such that:

- (1) For all  $n$ , the measure  $\lambda(\mathcal{U}_n)$  of  $\mathcal{U}_n$  is bounded by  $2^{-n}$ ; and
- (2) there is an  $\omega$ -c.e. function mapping  $n$  to a  $\Sigma_1^0$  index for  $\mathcal{U}_n$ .

A set (an element of Cantor space)  $X$  is captured by a Demuth test  $\langle \mathcal{U}_n \rangle$  if  $X \in \mathcal{U}_n$  for infinitely many  $n$ . A set is *Demuth random* if it is not captured by any Demuth test.

A set  $Z$  *weakly passes* a test  $\langle \mathcal{U}_n \rangle$  if  $Z \notin \bigcap_n \mathcal{U}_n$ . A set  $Z$  is *weakly Demuth random* if it weakly passes every Demuth test.

Figueira et al. [13] introduced balanced randomness, a notion in between weak Demuth randomness and ML-randomness where the  $m$ -th test component  $\mathcal{U}_m$  of a test can be “replaced” at most  $O(2^m)$  times. This notion



is still stronger than Oberwolfach randomness. More generally, for an order function  $h$  we say that  $Z$  is *h-weak Demuth random* if it weakly passes each Demuth test where the component  $\mathcal{U}_m$  can be replaced at most  $h(m)$  times.

It was observed in [3] that the methods of [13] show the following.

**Proposition 8.3.** *Let  $Z = Z_0 \oplus Z_1$  be ML-random. Then  $Z_0$  or  $Z_1$  is balanced random, and in fact  $O(r(n)2^n)$ -weak Demuth random for some order function  $r$ .*

*Proof.* We use the terminology of [13]. If  $Z_0$  is  $\omega$ -c.e. tracing then any weak Demuth test (which is given by an  $\omega$ -c.e. function) can be converted into a ML-test relative to  $Z_0$ . So by van Lambalgen theorem,  $Z_1$  is weak Demuth random.

If  $Z_0$  is not  $\omega$ -c.e. tracing then by [13, Thm. 23]  $Z_0$  is  $O(r(n)2^n)$ -weak Demuth random for some order function  $r$ , and in particular, balanced random.  $\square$

So weak weak König's lemma plus sufficient induction implies the axiom for balanced randomness.

**Definition 8.4.** For a computable function  $h$ , we say that a set  $Z$  is *h-c.e.* if there is a computable approximation such that  $Z \upharpoonright_n$  changes at most  $h(n)$  times. For instance, each left-c.e. set is  $2^n$ -c.e.

Such a set is clearly not *h-weak Demuth random*. So the following  $\omega$ -model  $\mathcal{M}$  satisfies WKL but not the axiom for weak *h*-Demuth randomness, for any function  $h$  that dominates each function  $\lambda n.k^n$ , such as  $h(n) = 2^{n \cdot p(n)}$  for some order function  $p$ .

**Proposition 8.5.** *There is an  $\omega$ -model  $\mathcal{M}$  of WKL such that each set of  $\mathcal{M}$  is superlow and  $k^n$ -c.e. for some  $k \in \mathbb{N}$ .*

*Proof.* Let  $\mathcal{S}(X)$  be the  $\Pi_1^0$  class relative to  $X$  of sets that are PA-complete in  $X$ . Over RCA, the axiom WKL is equivalent to  $\forall X \mathcal{S}(X) \neq \emptyset$ .

Let  $\mathcal{Q}$  be the  $\Pi_1^0$  class consisting of the sets  $Y$  such that  $Y_{i+1} \in \mathcal{S}(\bigoplus_{k \leq i} Y_k)$  for each  $i$ ; here  $Y_i = \{n : \langle i, n \rangle \in Y\}$  is the  $i$ -th column of  $Y$ . If  $Y \in \mathcal{Q}$  then the Turing ideal generated by the columns of  $Y$  determines an  $\omega$ -model  $\mathcal{M}$  of WKL.

Let  $X \rightarrow W^X$  be the c.e. operator such that

$$2^e(2n+1) \in W^X \Leftrightarrow \Phi_e^X(n) = 1\}.$$

By the superlow basis theorem as stated in [31, 1.8.38], but with the operator  $W$  instead of the domain of the usual Turing jump  $J$ , there is  $Y \in \mathcal{Q}$  such that  $W^Y$  is left-c.e.

Suppose that  $R = \Phi_e^Y$ . Since  $W^Y$  is left-c.e.,  $R$  is  $2^{2^e(2n+1)}$ -c.e., and hence  $k^n$ -c.e. where  $k = 2^{2^e+2}$ . Thus each set of  $\mathcal{M}$  is  $k^n$ -c.e. for some  $k \in \mathbb{N}$ .

Clearly  $Y' \leq_m W^Y$ . So  $Y$  is superlow.  $\square$

## 9. BELANGER, NIES AND SHAFER: THE STRENGTH OF RANDOMNESS EXISTENCE AXIOMS

David Belanger, André Nies and Paul Shafer others discussed the strength of randomness existence axioms at NUS and University of Ghent in February/March.



In [11, Section. 9], for a randomness notion  $\mathcal{C}$ , we defined  $\mathcal{C}_0$  to be the system  $\text{RCA} + \forall X \exists Y Y \in \mathcal{C}^X$ . For instance,  $\text{MLR}_0$  is equivalent to weak König's Lemma over  $\text{RCA}$ .

The system  $\text{CR}_0$  (computable randomness) appears to be equivalent to the seemingly weaker  $\text{SR}_0$  (Schnorr randomness) ([11, Prop. 9.2]; the strength of induction axioms that are needed to show this remains to be checked carefully).

**2-randomness versus weak 2-randomness.** On the other hand  $2\text{R}_0$  (the system for 2-randomness) is strictly stronger than  $\text{W2R}_0$  (the system for weak 2 randomness). To see this, take a weakly 2-random  $Z$  that does not compute a 2-random. For instance, any 2-random has hyperimmune degree. Any computably dominated ML-random  $Z$  is weakly 2-random and hence does not compute a 2-random. For each  $n$  let  $Z_n$  be the  $n$ -th column of  $Z$ , that is,  $Z_n = \{k : \langle k, n \rangle \in Z\}$ . Let  $\mathcal{M} = (\mathbb{N}, \mathcal{S})$  where  $\mathcal{S}$  consists of all the sets Turing below the join of finitely many columns of  $Z$ . Note that  $Z_n$  is weakly 2-random in any finite sum of columns not containing  $Z_n$ . So  $\mathcal{M}$  is a model of  $\text{W2R}_0$ .

We can also separate the two randomness existence axioms via an interesting mathematical consequence: Csima and Mileti [8] have shown that  $2\text{R}_0$  implies the Rainey Rambo's theorem.

**Proposition 9.1.**  *$\text{W2R}_0$  does not imply the Rainbow Ramsey's theorem.*

*Proof.* Joseph Miller has shown that the Rainbow Ramsey's theorem is equivalent over  $\text{RCA}_0$  plus some induction to the existence of a d.n.c. function relative to  $\emptyset'$ . (Detail needed here on the construction for the forward direction: recursive in a homogeneous set we obtain the function.) By [31, Exercise 4.3.18] there is a weakly 2-random set  $Z$  that does not compute a 2-fixed point free function, and hence it computes no d.n.c. function relative to  $\emptyset'$ . Construct the model  $\mathcal{M} \models \text{W2R}_0$  from  $Z$  as above. Then Rainbow Ramsey's theorem fails in  $\mathcal{M}$ .  $\square$

**Weak Demuth randomness versus WKL.**

**Definition 9.2.** A  $\Delta_2^0$  function  $f$  is  $\omega$ -c.e. if there is a computable function  $h$  such that  $h(n)$  bounds the number of changes in a computable approximation to  $f(n)$ .

A *Demuth test* is an effective sequence  $\langle \mathcal{U}_n \rangle$  of effectively open ( $\Sigma_1^0$ ) subsets of Cantor space such that:

- (1) For all  $n$ , the measure  $\lambda(\mathcal{U}_n)$  of  $\mathcal{U}_n$  is bounded by  $2^{-n}$ ; and
- (2) there is an  $\omega$ -c.e. function mapping  $n$  to a  $\Sigma_1^0$  index for  $\mathcal{U}_n$ .

A set (an element of Cantor space)  $X$  is captured by a Demuth test  $\langle \mathcal{U}_n \rangle$  if  $X \in \mathcal{U}_n$  for infinitely many  $n$ . A set is *Demuth random* if it is not captured by any Demuth test.

A set  $Z$  *weakly passes* a test  $\langle \mathcal{U}_n \rangle$  if  $Z \notin \bigcap_n \mathcal{U}_n$ . A set  $Z$  is *weakly Demuth random* if it weakly passes every Demuth test.

Figueira et al. [13] introduced balanced randomness, a notion in between weak Demuth randomness and ML-randomness where the  $m$ -th test component  $\mathcal{U}_m$  of a test can be “replaced” at most  $O(2^m)$  times. This notion

is still stronger than Oberwolfach randomness. More generally, for an order function  $h$  we say that  $Z$  is *h-weak Demuth random* if it weakly passes each Demuth test where the component  $\mathcal{U}_m$  can be replaced at most  $h(m)$  times.

It was observed in [3] that the methods of [13] show the following.

**Proposition 9.3.** *Let  $Z = Z_0 \oplus Z_1$  be ML-random. Then  $Z_0$  or  $Z_1$  is balanced random, and in fact  $O(r(n)2^n)$ -weak Demuth random for some order function  $r$ .*

*Proof.* We use the terminology of [13]. If  $Z_0$  is  $\omega$ -c.e. tracing then any weak Demuth test (which is given by an  $\omega$ -c.e. function) can be converted into a ML-test relative to  $Z_0$ . So by van Lambalgen theorem,  $Z_1$  is weak Demuth random.

If  $Z_0$  is not  $\omega$ -c.e. tracing then by [13, Thm. 23]  $Z_0$  is  $O(r(n)2^n)$ -weak Demuth random for some order function  $r$ , and in particular, balanced random.  $\square$

So weak weak König's lemma plus sufficient induction implies the axiom for balanced randomness.

**Definition 9.4.** For a computable function  $h$ , we say that a set  $Z$  is *h-c.e.* if there is a computable approximation such that  $Z \upharpoonright_n$  changes at most  $h(n)$  times. For instance, each left-c.e. set is  $2^n$ -c.e.

Such a set is clearly not *h-weak Demuth random*. So the following  $\omega$ -model  $\mathcal{M}$  satisfies WKL but not the axiom for weak *h*-Demuth randomness, for any function  $h$  that dominates each function  $\lambda n.k^n$ , such as  $h(n) = 2^{n \cdot p(n)}$  for some order function  $p$ .

**Proposition 9.5.** *There is an  $\omega$ -model  $\mathcal{M}$  of WKL such that each set of  $\mathcal{M}$  is superlow and  $k^n$ -c.e. for some  $k \in \mathbb{N}$ .*

*Proof.* Let  $\mathcal{S}(X)$  be the  $\Pi_1^0$  class relative to  $X$  of sets that are PA-complete in  $X$ . Over RCA, the axiom WKL is equivalent to  $\forall X \mathcal{S}(X) \neq \emptyset$ .

Let  $\mathcal{Q}$  be the  $\Pi_1^0$  class consisting of the sets  $Y$  such that  $Y_{i+1} \in \mathcal{S}(\bigoplus_{k \leq i} Y_k)$  for each  $i$ ; here  $Y_i = \{n : \langle i, n \rangle \in Y\}$  is the  $i$ -th column of  $Y$ . If  $Y \in \mathcal{Q}$  then the Turing ideal generated by the columns of  $Y$  determines an  $\omega$ -model  $\mathcal{M}$  of WKL.

Let  $X \rightarrow W^X$  be the c.e. operator such that

$$2^e(2n+1) \in W^X \Leftrightarrow \Phi_e^X(n) = 1\}.$$

By the superlow basis theorem as stated in [31, 1.8.38], but with the operator  $W$  instead of the domain of the usual Turing jump  $J$ , there is  $Y \in \mathcal{Q}$  such that  $W^Y$  is left-c.e.

Suppose that  $R = \Phi_e^Y$ . Since  $W^Y$  is left-c.e.,  $R$  is  $2^{2^e(2n+1)}$ -c.e., and hence  $k^n$ -c.e. where  $k = 2^{2^{e+2}}$ . Thus each set of  $\mathcal{M}$  is  $k^n$ -c.e. for some  $k \in \mathbb{N}$ .

Clearly  $Y' \leq_m W^Y$ . So  $Y$  is superlow.  $\square$

## 10. CARLUCCI: BOUNDED HINDMAN'S THEOREM AND INCREASING POLARIZED RAMSEY'S THEOREM

The following results were proved after reading the paper *Effectiveness of Hindman's Theorem for bounded sums* by Dzhafarov, Jockusch, Solomon and Westrick, [10].

The following natural restriction of Hindman's Theorem to sums with a bounded number of terms was discussed by Blass in [4] and first studied from a Reverse Mathematics perspective by Dzhafarov et alii in [10].

**Definition 10.1** (Hindman's Theorem with bounded sums).  $\text{HT}_k^{\leq n}$  states that for every coloring  $f : \mathbb{N} \rightarrow k$  there exists an infinite set  $H$  such that  $FS^{\leq n}(H)$  is monochromatic for  $f$ , where  $FS^{\leq n}(H)$  denotes the set of all finite sums of at most  $n$  distinct members of  $H$ . We denote  $\forall k \text{ HT}_k^{\leq n}$  by  $\text{HT}^{\leq n}$ .

The main results in [10] are (1) that  $\text{HT}_2^{\leq 2}$  is unprovable in  $\text{RCA}_0$  and (2) that  $\text{HT}_3^{\leq 3}$  proves  $\text{ACA}_0$  over  $\text{RCA}_0$ .

The following version of Ramsey's Theorem is introduced in [9].

**Definition 10.2** (Increasing Polarized Ramsey Theorem).  $\text{IPT}_k^n$  is the following principle: for every  $f : [\mathbb{N}]^n \rightarrow k$  there exists a sequence  $\langle H_1, \dots, H_n \rangle$  of infinite sets and  $c < k$  such that for all increasing tuple  $(x_1, \dots, x_n) \in H_1 \times \dots \times H_n$  we have  $f(x_1, \dots, x_n) = c$ . The sequence  $\langle H_1, \dots, H_n \rangle$  is called increasing p-homogeneous for  $f$ . We denote  $\forall k \text{ IPT}_k^n$  by  $\text{IPT}^n$ .

We first prove that  $\text{HT}_5^{\leq 2}$  implies  $\text{IPT}_2^2$  over  $\text{RCA}_0$  by a direct combinatorial argument.

**Proposition 10.3.**  $\text{RCA}_0 \vdash \text{HT}_5^{\leq 2} \rightarrow \text{IPT}_2^2$

*Proof.* We use the following notation: for  $n \in \mathbb{N}$ , if  $n = i_0 \cdot 3^{k_0} + \dots + i_t \cdot 3^{k_t}$  with  $k_0 < \dots < k_t$  and  $i_0, \dots, i_t \in \{1, 2\}$ , we denote  $k_0$  by  $\lambda(n)$ ,  $k_t$  by  $\mu(n)$ , and  $i_0$  by  $i(n)$ . The following elementary properties hold (see [10], Theorem 3.1):

- (P1) If  $\lambda(n) < \lambda(m)$  then  $\lambda(n + m) = \lambda(n)$  and  $i(n + m) = i(n)$ .
- (P2) If  $\lambda(n) = \lambda(m)$  and  $i(n) = i(m) = 1$  then  $\lambda(n + m) = \lambda(n)$  and  $i(n + m) = 2$ .
- (P3) If  $\lambda(n) = \lambda(m)$  and  $i(n) = i(m) = 2$  then  $\lambda(n + m) = \lambda(n)$  and  $i(n + m) = 1$ .
- (P4) If  $\mu(n) < \mu(m)$  then  $\lambda(n + m) = \lambda(n)$  and  $\mu(n + m) = \mu(m)$ .

Let  $f : [\mathbb{N}]^2 \rightarrow 2$  be given. Define  $g : \mathbb{N} \rightarrow 5$  as follows.

$$g(n) := \begin{cases} 0 & \text{if } n = i \cdot 3^t, i \in \{1, 2\}, \\ 1 + f(\lambda(n), \mu(n)) & \text{if } n \neq i \cdot 3^t \wedge i(n) = 1, \\ 3 + f(\lambda(n), \mu(n)) & \text{if } n \neq i \cdot 3^t \wedge i(n) = 2. \end{cases}$$

Note that  $g$  is well-defined since  $\lambda(n) < \mu(n)$  if  $n$  is not of the form  $i \cdot 3^t$ ,  $i \in \{1, 2\}$ .

Let  $H$  witnessing  $\text{HT}_5^{\leq 2}$  for  $g$  be an infinite set such that  $FS^{\leq 2}(H)$  is monochromatic under  $g$ .

First, the color of  $FS^{\leq 2}(H)$  cannot be 0: the set  $H$  cannot contain two terms  $3^p, 3^q$  with  $p < q$  since their sum is not of the form  $i \cdot 3^r$ , and it cannot contain two terms  $2 \cdot 3^p, 2 \cdot 3^q$  with  $p < q$  since their sum is not of the form  $i \cdot 3^r$ .

Second, for all  $h, h' \in FS^{\leq 2}(H)$ ,  $i(h) = i(h')$ :<sup>1</sup>  $i(n) = 1$  implies  $g(n) \in \{1, 2\}$  and  $i(n) = 2$  implies  $g(n) \in \{3, 4\}$ . Then also the following property (P6) holds under the assumption that  $FS^{\leq 2}(H)$  (rather than  $FS^{\leq 3}(H)$ , as in [10]) is monochromatic for  $g$ : for all  $k \geq 0$  there is at most one  $n \in H$  such that  $\lambda(n) = k$ . Suppose otherwise as witnessed by  $h \neq h'$  in  $H$  with  $\lambda(h) = \lambda(h')$ . Since we also have  $i(h) = i(h')$ , it follows that  $i(h + h') \neq i(h) = i(h')$ , contra (P5).

Hence we can sparsify  $H$  (computably) so as to ensure the following

(Apartness Condition): if  $h < h'$  are in  $H$  then  $\mu(h) < \lambda(h')$ .

Assume without loss of generality that  $H$  satisfies the apartness condition. Assume without loss of generality that the value  $i(h)$  for  $h \in H$  is 1. Let  $c \in \{1, 2\}$  be such that  $FS^{\leq 2}(H)$  has color  $c$  under  $g$ .

Let

$$H_1 := \{\lambda(n) : n \in H\}$$

and

$$H_2 := \{\mu(n) : n \in H\}.$$

We claim that  $\langle H_1, H_2 \rangle$  is increasing p-homogeneous for  $f$ .

First observe that, letting  $H = \{h_1, h_2, \dots\}_<$ , we have  $H_1 = \{\lambda(h_1), \lambda(h_2), \dots\}_<$  and  $H_2 = \{\mu(h_1), \mu(h_2), \dots\}_<$ . This is so because  $\lambda(h_1) < \mu(h_1) < \lambda(h_2) < \mu(h_2) < \dots$  by the apartness condition and the fact that the color is not 0.

Then we claim that  $f(x_1, x_2) = c - 1$  for every increasing pair  $(x_1, x_2) \in H_1 \times H_2$ . Note that  $(x_1, x_2) = (\lambda(h_i), \mu(h_j))$  for some  $i \leq j$ . If  $i = j$  we have

$$c = g(h_i) = 1 + f(\lambda(h_i), \mu(h_i)),$$

and if  $i < j$  we have

$$c = g(h_i + h_j) = 1 + f(\lambda(h_i + h_j), \mu(h_i + h_j)) = 1 + f(\lambda(h_i), \mu(h_j)),$$

since  $FS^{\leq 2}(H)$  is monochromatic for  $g$  with color  $c$ . Thus, in any case

$$c = 1 + f(\lambda(h_i), \mu(h_j)) = 1 + f(x_1, x_2).$$

This shows that  $\langle H_1, H_2 \rangle$  is increasing p-homogeneous of color  $c - 1$  for  $f$ .  $\square$

**Discussion.** Proposition 10.3 should be compared with Corollary 2.4 of [10]:  $\text{RCA}_0 + B\Sigma_2^0 + \text{IPT}_2^2 \vdash \text{SRT}_2^2$ . Proposition 10.3 has the following corollaries.

**Corollary 10.4.** *Over  $\text{RCA}_0$ ,  $\text{HT}_5^{\leq 2}$  implies  $\text{SRT}_2^2$ .*

*Proof.* Dzhafarov and Hirst show that  $\text{IPT}_2^2$  implies  $\text{D}_2^2$  over  $\text{RCA}_0$  (Proposition 3.5 in [9]). Chong, Lempp and Yang have later proved that  $\text{D}_2^2$  implies  $\text{SRT}_2^2$  over  $\text{RCA}_0$  (Theorem 1.4 in [6]).  $\square$

Since  $\text{SRT}_2^2$  implies  $B\Sigma_2^0$ , we also have the following corollary.

**Corollary 10.5.**  *$\text{HT}_5^{\leq 2}$  is not provable in  $\text{WKL}_0$ .*

<sup>1</sup>This is Property (P5) of [10] strengthened to  $FS^{\leq 2}(H)$  instead of  $H$ . Note that this is necessary for its application just below establishing (P6), and the same is true in the setting of [10], which needs a minor correction.

Also, as Ludovic Patey kindly pointed out to us,  $\text{IPT}_2^2$  is known to be *strictly* stronger than  $\text{SRT}_2^2$ : Theorem 2.2 in [7] showed that there is a non-standard model of  $\text{SRT}_2^2 + \text{B}\Sigma_2^0$  having only low sets in the sense of the model. Lemma 2.5 in [9] can be formalized in  $\text{RCA}_0$  and shows that no model of  $\text{IPT}_2^2$  can contain only  $\Delta_2^0$  sets. Thus, Proposition 10.3 implies that  $\text{HT}_5^{\leq 2}$  is strictly stronger than  $\text{SRT}_2^2$ .

The proof of Proposition 10.3 is easily adapted to show

$$\text{RCA}_0 \vdash \forall n (\text{HT}_{2n+1}^{\leq 2} \rightarrow \text{IPT}_n^2).$$

Then  $\text{RCA}_0 \vdash \text{HT}^{\leq 2} \rightarrow \text{IPT}^2$ . On the other hand we know that  $\text{IPT}^2 \rightarrow \text{SRT}^2$ , where  $\text{SRT}^2$  denotes the Stable Ramsey's Theorem for pairs and all colors (Dzhafarov and Hirst [9], Theorem 3.3). Finally, it is known that  $\text{RCA}_0 + \text{SRT}^2 \vdash \text{B}\Sigma_3^0$  (Cholak, Jockusch and Slaman [33], Section 11.2). Therefore we also have the following corollary.

**Corollary 10.6.** *Over  $\text{RCA}_0$ ,  $\text{HT}^{\leq 2}$  implies  $\text{B}\Sigma_3^0$ .*

The author has been up to now unable to lift the combinatorial argument in the proof of Proposition 10.3 to show that  $\text{HT}_k^{\leq 3}$  implies  $\text{IPT}_2^3$ , for some  $k \geq 2$ . Note that by results of [9] and [10] the following holds:  $\text{RCA}_0 \vdash \text{HT}_4^{\leq 3} \rightarrow \text{IPT}_2^3$ .

## Part 5. Computational complexity theory

### 11. THOMPSON: SYMMETRIC FUNCTIONS CAN BE COMPUTED BY BOOLEAN CIRCUITS OF LINEAR SIZE AND LOGARITHMIC DEPTH

Declan Thompson and Matt Bray, Honour's students from Auckland University, visited the Research Centre Coromandel in February. Declan worked on Boolean circuits, connecting to the CompSci 750 class on computational complexity which André had co-taught in Semester 2, 2015.

A function  $f: \{0, 1\}^n \rightarrow \{0, 1\}$  is symmetric if its value does not depend on the order of its arguments. For Boolean symmetric functions, this means that the output depends only on the number of 1s in the input. It is not hard to see that given a binary representation of the number of 1s in the input, a Boolean circuit of linear size and logarithmic depth can compute the value of a symmetric function. So it suffices to find an efficient method for obtaining this binary representation from the original input.

Circuits exist which add binary numbers in linear size and logarithmic depth (see, for example, the Krapchenko adder of [43]). A naïve approach to counting the number of 1s is to treat each input as an individual number and utilise an adding tree. Unfortunately this requires a circuit of more than logarithmic depth. Instead, we will utilise so called “3-for-2” adders and finally only one Krapchenko adder.

A *full adder* is a circuit for calculating the sum of three bits. Figure 1 gives a construction for a full adder. There are three input bits and two output bits, representing the two bit output. A *carry save adder* (CSA) utilises a chain of full adders to take three  $n$ -bit inputs  $a, b, c$  and return two  $n + 1$ -bit outputs  $u, v$  such that  $a + b + c = u + v$ . The CSA works by

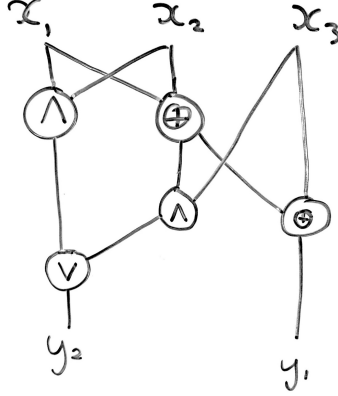


FIGURE 1. A full adder.  $x_1 + x_2 + x_3 = y_2y_1$ .  $\oplus$  denotes addition modulo 2.

sending sum bits ( $y_1$  in Figure 1) to  $u$  and carry bits ( $y_2$ ) to  $v$ . Specifically, if the full adder returns  $y_2y_1$  from  $a_i, b_i, c_i$ , then  $u_i = y_1$  and  $v_{i+1} = y_2$ . We set  $u_n = v_0 = 0$ . As an example, consider the following sum.

$$\begin{array}{r}
 100110 \\
 111101 \\
 + 101101 \\
 \hline
 0110110 = u \\
 1011010 = v
 \end{array}$$

A full adder has a constant number of gates and a CSA uses a full adder for each bit. Hence a CSA uses  $O(n)$  size circuits with depth constant, where  $n$  is the number of bits of each input number.

We construct an adder tree for  $x_0, \dots, x_{n-1}$  by running CSAs in parallel and then combining their outputs. At the first “level”, there are  $\frac{1}{3}n$  CSAs each taking in three 1 bit inputs and returning two 2 bit outputs (4 wires in total). At the second level there are  $\frac{1}{3}n \cdot 2$  total inputs and each CSA takes three inputs, so there are  $\frac{1}{3} \cdot \frac{2}{3}n$  CSAs. In general, at the  $j$ th level there are  $\frac{1}{3} \cdot \frac{2^{j-1}}{3}n$  CSAs taking three  $j$  bit inputs and returning two  $j+1$  bit outputs. Each CSA decreases the number of numbers to add by 1 until we are left with two binary numbers. Hence we require  $n-2$  CSAs.

Logarithmic depth of the adder tree is easy to establish. Each CSA has constant depth and since we combine them in a tree fashion the depth of CSAs is logarithmic. Each CSA has size proportional to the number of bits in the inputs. From this, we can conclude that the size of the adder tree is approximately

$$O\left(\frac{1}{3}n \sum_{j=1}^{\lfloor \log n \rfloor} \frac{2^{j-1}}{3} j\right).$$

However  $\sum_{j=1}^{\infty} \frac{2^{j-1}}{3} j = 9$  and so in fact the adder tree is of size  $O(n)$ .

Thus we have obtained two binary numbers which add to the total number of 1s in the input, using linear size and logarithmic depth circuits. It is

now a simple process to use a linear size, logarithmic depth adder (such as Krapchenko's) to obtain a single binary number, which can then be used to determine the output of an arbitrary symmetric function.

## 12. DESCRIBING ORDINALS LESS THAN $\varepsilon_0$ BY FINITE TREES

Andreas Weiermann, Paul Shafer and Nies discussed in Ghent in March. This discussion connected some well-known facts.

For this note a *tree*  $B$  is an acyclic connected directed finite graph with a distinguished root  $r$ .  $B$  can be naturally viewed as a finite subset of  $\omega^{<\omega}$  (sequences of natural numbers) closed under initial segments;  $r$  is the empty string. If  $B \neq r$  then  $B$  is given by a tuple  $(B_1, \dots, B_n)$  of trees, where the  $B_i$  correspond to the successors of  $r$  from left to right.

The ordinal  $o(B)$  is defined recursively as follows: let  $o(r) = 0$ . If  $B = (B_1, \dots, B_n)$  then

$$o(B) = \sum_{i=1}^n \omega^{o(B_{\pi(i)})}$$

where  $\pi$  is a permutation of  $\{1, \dots, n\}$  such that  $o(B_{\pi(1)}) \geq \dots \geq o(B_{\pi(n)})$ .

The *norm*  $N(\alpha)$  of an ordinal  $\alpha < \varepsilon_0$  is defined by  $N(0) = 0$  and  $N(\gamma) = 1 + N(\alpha) + N(\beta)$  if  $\gamma$  has Cantor normal form  $\omega^\alpha + \beta$ . Clearly each  $\gamma < \varepsilon_0$  has the form  $o(B)$  for some tree  $B$ , and  $N(\gamma)$  is the number of edges of such a tree.

The ordinal of a tree is a complete invariant for tree isomorphism:

**Proposition 12.1.** *Let  $B, C$  be trees. We have*

$$B \cong C \Leftrightarrow o(B) = o(C).$$

*Proof.* First suppose that  $\rho: B \cong C$ . If  $B = C = r$  then  $o(B) = o(C) = 0$ . Otherwise  $B = (B_1, \dots, B_n)$ ,  $C = (C_1, \dots, C_n)$  and  $\rho: B_i \cong C_{\sigma(i)}$  for  $\sigma \in S_n$ . Inductively we have  $o(B_i) \cong o(C_{\sigma(i)})$ . Choose  $\pi \in S_n$  such that  $o(B_{\pi(1)}) \geq \dots \geq o(B_{\pi(n)})$ . Then  $o(C_{\sigma(\pi(1))}) \geq \dots \geq o(C_{\sigma(\pi(n))})$ . Therefore  $o(B) = o(C)$ .

Now suppose  $\alpha = o(B) = o(C)$ . If  $\alpha = 0$  we have  $B \cong C$  trivially. Otherwise write  $\alpha$  in Cantor normal form  $\sum_{i=1}^n \omega^{\beta_i}$  where  $\beta_1 \geq \dots \geq \beta_n$ . Since CNF is unique we have  $B = (B_1, \dots, B_n)$ ,  $C = (C_1, \dots, C_n)$  with  $\beta_i = o(B_{\pi(i)}) = o(C_{\theta(i)})$  for  $\pi, \theta \in S_n$ . This shows that  $B \cong C$ .  $\square$

The number of ordinals  $\alpha$  with  $N(\alpha) = n$  is asymptotically  $(2.95)^n n^{-1.5}$  by a result of Weiermann. The number of trees with  $n$  edges is  $\binom{2n}{n}/(n+1)$  (Catalan number), which is asymptotically  $4^n n^{-1.5}/\sqrt{\pi}$  (much larger).

A tree  $B$  is canonical if  $B$  is a root, or  $B = (B_1, \dots, B_n)$  for canonical trees  $B_i$  such that  $o(B_1) \geq \dots \geq o(B_n)$ . Clearly each ordinal less than  $\varepsilon_0$  is  $o(B)$  for a unique canonical tree. Isomorphism and canonization is in LOGSPACE by a result of Aho, Hopcroft and Ullman. Also see Buss 1995 where algorithms in the smaller class ALOGSPACE are given.

**Question 12.2.** *How can one generate a random ordinal with given norm  $n$  using  $\text{poly}(n)$  steps and the appropriate number of  $n \log_2(2.95)$  of random bits?*

This amounts to generating a random canonical tree with  $n$  edges.

## 13. NIES AND SCHOLZ: GROTHENDIECK'S CONSTANTS

(Written by Nies after some discussion with Volkher Scholz, who works at U Gent in the research group of Prof. Verstraete, and visited Auckland in April.) Let  $\mathbb{F}$  be one of the fields  $\mathbb{R}, \mathbb{C}$ . Choose scalars from  $\mathbb{F}$ . A. Grothendieck proved in 1953 that there are positive constants  $K_G^{\mathbb{F}}$  as follows.

Let  $C = \langle \gamma_{i,k} \rangle$  be an  $n \times n$  matrix such that

$$(13.1) \quad \sum_{i,k} \gamma_{i,k} a_i b_k \leq \sup_i |a_i| \sup_k |b_k|$$

for each scalars  $a_i, b_k$ . Then for each Hilbert space  $H$  over  $\mathbb{F}$ , and vectors  $x_i, y_k \in H$  ( $1 \leq i, k \leq n$ )

$$\sum_{i,k} \gamma_{i,k} \langle x_i, y_k \rangle \leq K_G^{\mathbb{F}} \sup_i \|x_i\| \sup_k \|y_k\|.$$

See the reprinted paper [19]. In (13.1) we may assume that  $|a_i| = |b_k| = 1$  because for fixed  $C$  the inequality describes a convex set, so it suffices to look at its extreme points. Given the matrix  $C$  as an input, it is known, that the condition is NP-hard. Say for  $\mathbb{R}$  the problem Max-Cut can be reduced to it (which asks given a graph whether one can partition the set of vertices into two sets so that the number of crossing edges is above a threshold). Easy matrices  $C$  satisfying the condition are:  $n^{-1}I$ , or the one where each  $\gamma_{i,k}$  equals  $n^{-2}$ .

We can get away with finite-dimensional Hilbert spaces. However the dimension of  $H$  must be unbounded. E.g the value of  $K_G^{\mathbb{R}}$  for dimension 2 is  $\sqrt{2}$ .

Interestingly, G's work is closely related to, but predated the Bell inequality (1964). The transition from a problem in real analysis to the setting of Hilbert space corresponds to the transition from classical to quantum physics. The real Grothendieck constant can be viewed as an upper bound on the possible violation of Bell's inequality in a quantum system.

The precise values of the constants are not known. We know that (see [34])

$$1 < K_G^{\mathbb{C}} < K_G^{\mathbb{R}} < 1.782.$$

Raghavendra and Steurer [36, Thm 1.3] prove that  $K_G^{\mathbb{R}}$  is a computable real, and in fact computable up to precision  $\eta > 0$  in time proportional to  $\exp(\exp(O(\eta^{-3})))$ . No surprise we still don't know what its value is.

## Part 6. Group theory and its connections to logic

## 14. DOUCHA AND NIES: PRIMITIVE GROUP ACTIONS IN THE SETTING OF POLISH SPACES

Michal Doucha and Nies worked at the RCC in 2014/2015.

**Definition 14.1.** Let  $G$  be a Polish group and  $X$  a Polish  $G$ -space with all orbits dense.  $(G, X)$  is called *imprimitive* if there exists a closed proper subset  $D \subseteq X$  such that for every  $g \in G$  either  $g \cdot D = D$  or  $g \cdot D \cap D = \emptyset$  and moreover,  $D$  intersects some orbit in at least two elements. I.e.,  $\exists x \neq y \in D \exists g \in G [g \cdot x = y]$ . The set  $D$  is called a *closed domain of imprimitivity*. Otherwise,  $(G, X)$  is called *primitive*.



Given an action  $G \curvearrowright X$ , we say that an equivalence relation  $E$  on  $X$  is  $G$ -invariant if for every  $g \in G$  and every  $x, y \in X$  we have  $xEy \leftrightarrow g \cdot xEg \cdot y$ . Equivalently,  $g \cdot [x]_E = [g \cdot x]_E$  for each  $g \in G$  and  $x \in X$ .

**Proposition 14.2.** *Given a Polish group  $G$  and a Polish  $G$ -space  $X$  with all orbits dense, TFAE:*

- (i)  $(G, X)$  is imprimitive
- (ii) there exists a  $G$ -invariant smooth equivalence relation  $E$  on  $X$  other than  $\text{id}_X$  or  $X^2$ , with all equivalence classes closed, such that some equivalence class intersects some orbit in at least two elements.
- (iii) as in (ii) but without the restriction to smoothness.

*Proof.* (iii)  $\rightarrow$  (i) Let  $D = [x]_E$  be an equivalence class of  $E$  that intersects some orbit in at least two points. We claim that  $D$  is a closed domain of imprimitivity. It is clearly closed and properly contained in  $X$ . For each  $g \in G$ , if  $gxEx$  we have  $gD = [gx]_E = D$ . Otherwise  $gD \cap D = \emptyset$ .

(i)  $\rightarrow$  (ii). Let  $D$  be a closed domain of imprimitivity. Let

$$H = \{h \in G : h \cdot D = D\}.$$

Clearly,  $H$  is a closed subgroup of  $G$ . Since every orbit in  $X$  is dense and  $D$  is a proper subset,  $H$  is a proper subgroup of  $G$ .

Let us define a relation  $E$  on  $X$ . For  $x, y \in X$  we define

$$xEy \leftrightarrow \exists g \in G [g^{-1} \cdot x \in D \wedge g^{-1} \cdot y \in D].$$

We shall prove that  $E$  is a smooth  $G$ -invariant equivalence relation with closed classes such that some class intersects some orbit in at least two elements.

Since for every  $g \in G$  the map  $x \rightarrow g \cdot x$  is a homeomorphism of  $X$  we have that for each  $g \in G$  the set  $g \cdot D$  is also closed. Denote by  $X/D$  the set  $\{g \cdot D : g \in G\}$ . We claim for every  $F_1 \neq F_2 \in X/D$  we have  $F_1 \cap F_2 = \emptyset$ . Indeed, write  $F_i$  as  $g_i \cdot D$  for  $g_i \in G$ , where  $i \in \{1, 2\}$ . If  $g_1 \cdot D \cap g_2 \cdot D \neq \emptyset$ , then  $D \cap (g_1^{-1} \cdot g_2) \cdot D \neq \emptyset$ . Thus by assumption  $(g_1^{-1} \cdot g_2) \cdot D = D$ , so  $g_1 \cdot D = g_2 \cdot D$ , a contradiction. It follows that  $X/D$  is the set of  $E$ -classes. In particular,  $E$  is an equivalence relation with each equivalence class being closed and the  $E$ -class  $D$  intersects by assumption some orbit in at least two elements.

Consider the quotient  $G/H$  consisting of left cosets of  $H$  with the quotient topology. It is a folklore fact that this is a Polish space metrizable by the metric  $\delta$  defined for any  $g_1 \cdot H, g_2 \cdot H$  as the Hausdorff distance

$$\delta(g_1 \cdot H, g_2 \cdot H) = \inf\{d_G(h_1, h_2) : h_1 \in g_1 \cdot H, h_2 \in g_2 \cdot H\},$$

where  $d_G$  is some compatible right-invariant metric on  $G$ . See for example [16] for details. Let us define the map  $\phi : X \rightarrow G/H$  as follows:

$$\phi(x) = g \cdot H \text{ if } g^{-1} \cdot x \in D.$$

This is well-defined since  $H$  fixes  $D$ . We now claim that  $\phi$  is a Borel reduction of  $E$  into  $\text{id}(G/H)$ . This will show that  $E$  is smooth.

To show that it is a reduction, pick some  $x, y \in X$ . Suppose that  $xEy$ . Then by definition there is  $g \in G$  such that  $g^{-1} \cdot x$  and  $g^{-1} \cdot y$  lie in  $D$ , thus

$\phi(x) = \phi(y) = g \cdot H$ . On the other hand, if  $\phi(x) = \phi(y) = g \cdot H$ , then  $g^{-1} \cdot x$  and  $g^{-1} \cdot y$  lie in  $D$ .

It remains to check that  $\phi$  is Borel. We show that  $\phi$  factorizes through  $X/D$  as  $\psi \circ \pi$ , where  $\pi : X \rightarrow X/D$  is the canonical projection and  $\psi : X/D \rightarrow G/H$  sends  $g \cdot D$  to  $g \cdot H$ . We note that a set  $U \subseteq X/D$  is open if and only if  $\bigcup U$  is open in  $X$ . Then we show that  $\psi$  is continuous (even open) and  $\psi$  is a bijection whose inverse  $\psi^{-1}$  is continuous, that suffices.

That  $\pi$  is continuous (and open) follows directly from the definition of the topology on  $X/D$ . Also, it is clear that  $\psi$  is a bijection. We check that  $\psi^{-1}$  is continuous. Let  $U \subseteq X/D$  be an open neighbourhood of some  $g \cdot D$ . Pick arbitrarily some  $x \in D$ . Since  $\bigcup U$  is an open neighbourhood of  $x$  and the group action is continuous there exists an open neighbourhood  $V$  of  $g$  such that for every  $h \in V$  we have  $h \cdot x \in \bigcup U$ . We have that  $V_H = V \cdot H$  is an open neighbourhood of  $g \cdot H$  in  $G/H$  and we claim that  $\psi^{-1}(V_H) \subseteq U$ . This is immediate. Any element of  $V_H$  is of the form  $h \cdot H$  for some  $h \in V$  and thus sent by  $\psi^{-1}$  to  $h \cdot D$ . We have that  $h \cdot x \in \bigcup U$  and since  $\bigcup U$  is  $E$ -invariant we have that  $h \cdot D \subseteq \bigcup U$ , thus  $h \cdot D \in U$ .  $\square$

**Proposition 14.3.** *Let  $G$  be a Polish group and  $X$  a Polish  $G$ -space with all orbits dense. Suppose that for any  $x \in X$  the stabilizer  $G_x$  is a maximal closed subgroup of  $G$ . Then  $(G, X)$  is primitive.*

*Proof.* Suppose that  $(G, X)$  is imprimitive, so there exists a closed domain of imprimitivity  $D \subseteq X$ . Let  $H = \{h \in G : h \cdot D = D\}$ .  $H$  is clearly a closed subset of  $G$ . Moreover, since  $D$  is a closed domain of imprimitivity we have that  $H$  is a group. Let  $x \in X$  be such that we have  $|D \cap G \cdot x| \geq 2$ . We may suppose that  $x \in D$ . We have that  $G_x \leq H$ . We shall show that  $G_x < H < G$  and that will be a contradiction with the maximality of  $G_x$ . By assumption there exists  $h \in G \setminus G_x$  such that  $h \cdot x \in D$ . Since  $D$  is a domain of imprimitivity, so for every  $g \in G$  we have either  $g \cdot D = D$  or  $g \cdot D \cap D = \emptyset$ , we must have that  $h \cdot D = D$  and thus  $h \in H$ . We have shown that  $G_x < H$ . On the other hand,  $D$  is a proper closed subset of  $X$  and since the orbit of  $x$  is dense, there exists  $g \in G$  such that  $g \cdot x \notin D$  and thus  $g \cdot D \cap D = \emptyset$  and  $g \notin H$ . We have shown that  $H < G$  and the proof is complete.  $\square$

### Questions.

1. How about the converse implication in Prop. 14.3?
2. Robinson [38, 7.2.5] states that if  $G$  is primitive on  $X$ , then every nontrivial normal subgroup is transitive. (The latter property is called quasiprimitive by Cheryl Praeger.) Check this in the Polish setting, where the normal subgroup is closed, and we have topological transitivity in that every orbit is dense.

### 15. NIES AND TENT: A SENTENCE OF SIZE $O(\log n)$ EXPRESSING THAT A GROUP HAS $n$ ELEMENTS

This post is related to Nies' and Tent's article "Describing finite groups by short first-order sentences" [32]. We use the definition  $\log n = \min\{r : 2^r \geq n\}$ . In that article we gave a description of any finite group  $G$  via a first order sentence of length  $O(\log^3 |G|)$ . Here we want to express that the group

has size  $n$  by a first-order sentence of length  $O(\log n)$ . This will also yield a new way to describe the finite simple groups in length  $O(\log n)$ , still relying on CFSG but not relying on the short presentations in [20]

This work happened in March 2016 at UCLA, after some preliminary work of Nies with the honour's student Matthew Bray. At the BIRS permutation groups meeting Nov 13-18, Csaba Schneider and David Craven provided the crucial references needed to distinguish by short first order sentences the few examples of non isomorphic simple groups of the same size.

**Theorem 15.1.** *For each  $n$  there is a sentence  $\phi_n$  in the first order language of groups such that  $|\phi_n| = O(\log n)$  and for each group  $G$ ,*

$$G \models \phi_n \Leftrightarrow |G| = n.$$

We first provide some necessary facts. We use [32, Lemma 2.1]:

**Lemma 15.2.** *For each positive integer  $r$ , there is an existential formula  $\theta_r(g, x)$  in the first-order language of monoids  $L(e, \circ)$ , of length  $O(\log r)$ , such that for each monoid  $M$ ,  $M \models \theta_r(g, x)$  if and only if  $x^r = g$ .*

In particular, we can express that a group  $G$  has exponent dividing  $r$  using  $O(\log r)$ . The following variant is also needed.

**Lemma 15.3.** *For each positive integer  $k$ , there is a formula  $\psi_r(y, x)$  in the first-order language of monoids  $L(e, \circ)$ , of length  $O(\log r)$ , such that for each monoid  $M$ ,  $M \models \psi_r(g, x)$  if and only if  $x^i = g$  for some  $i$  with  $0 \leq i \leq r$ .*

*Proof.* Let  $\psi_1(y, x) \equiv y = 1 \vee y = x$ . Recursively define

$$\psi_{2k}(y, x) \equiv \exists u, v [y = uv \wedge \forall z. (z = u \vee z = v) \psi_k(z, x)]$$

$$\psi_{2k+1}(y, x) \equiv \exists u, v [(y = uv \vee y = uvx) \wedge \forall z. (z = u \vee z = v) \psi_k(z, x)]$$

Clearly  $\psi_r$  works as required. Further,  $|\psi_r| = O(\log r)$ .  $\square$

We next provide an easy fact on  $p$ -groups (which is not first order at this stage).

**Fact 15.4.** *Suppose  $L$  is a  $p$ -group. Then  $|L| \leq p^r \Leftrightarrow \exists x_1, \dots, \exists x_r \in L \forall y \in L$*

$$(\diamond) \quad \exists a_1, \dots, a_r [0 \leq a_i < p \wedge y = \prod_i x_i^{a_i}].$$

*Proof.* The implication  $\Leftarrow$  is immediate.

For the implication  $\Rightarrow$ , we use induction on  $r$ . The base case  $r = 1$  is obvious since  $L$  is trivial or cyclic of order  $p$ . Now suppose  $r > 1$  and the implication holds for  $r - 1$ . If  $L$  is non-trivial, pick  $x_r$  in the centre of order  $p$ . By inductive hypothesis for  $L/N$  where  $N = \langle x_r \rangle$ , we can choose  $x_1, \dots, x_{r-1} \in L$  such that statement holds in  $L/N$  via  $x_i N$ ,  $1 \leq i < r$ . So for each  $y \in L$ , we have

$$yN = \prod_{i=1}^{r-1} (x_i N)^{a_i} = \prod_{i=1}^{r-1} (x_i)^{a_i} N$$

for some  $a_i$  with  $0 \leq a_i < p$ . Therefore there is  $a_r$  with  $0 \leq a_r < p$  such that  $y = \prod_i x_i^{a_i}$ , as required.  $\square$

**Lemma 15.5.** *For  $k = p^r$ ,  $p$  prime,  $r \in \mathbb{N}$  there is a sentence  $\beta_k$  of length  $O(\log k)$  such that  $G \models \beta_k$  iff  $G$  has a subgroup of size  $k$ .*

*Proof.* We express  $(\diamond)$  by a first-order sentence of length  $O(\log k)$  via the formulas in Lemma 15.3:

$$\begin{aligned} \chi_k(y; x_1, \dots, x_r) &\equiv \exists s_0, \dots, s_r \\ &\quad [s_0 = 1 \wedge s_r = y \wedge \bigwedge_{i=1}^r \exists v (\psi_{p-1}(v, x_i) \wedge s_i = s_{i-1}v)]. \end{aligned}$$

The length of  $|\chi_k|$  is  $O(r \log p) = O(\log k)$ .

Given a group  $G$  and  $\bar{x} = x_1, \dots, x_r \in G$ , write  $U_{\bar{x}}^k = \{y \in G : G \models \chi_k(y; \bar{x})\}$ . The sentence  $\beta_k$  expresses that there is  $\bar{x} = x_1, \dots, x_r$  such that  $U_{\bar{x}}^k$  is a subgroup of exponent dividing  $k$ , and  $r$  is optimal, namely, there is no  $\bar{y} = y_1, \dots, y_{r-1}$  such that  $U_{\bar{y}}^{k/p} = U_{\bar{x}}^k$ .

If  $G$  has a subgroup  $L$  of size  $k$  then  $G \models \beta_k$  by Fact 15.4. Now suppose  $G \models \beta_k$  via  $x_1, \dots, x_r \in G$ . Then  $L = U_{\bar{x}}^k$  is a subgroup of  $G$  of size  $k$ .  $\square$

*Proof of Thm. 15.1.* Using Lemma 15.2 we can express that the group  $G$  has exponent dividing  $n$ . In particular, only prime factors of  $n$  can occur in the order of  $G$ . Suppose  $n = \prod_{i=1}^m p_i^{r_i}$  for prime numbers  $p_1, \dots, p_m$ . We express using Lemma 15.5 for each  $i \leq m$  that there is a Sylow subgroup of size  $p_i^{r_i}$ . For each  $i$  this takes length  $O(\log(p_i^{r_i}))$  with the  $O$ -constant independent of  $i$ . So the resulting sentence has length  $O(\log n)$ .  $\square$

It would be interesting to find sentences as in Theorem 15.1 with a bounded number of quantifier alternations.

Next we express in logarithmic length that a group is simple. We use [32, Lemma 2.3] on generation. The notation is adapted slightly.

**Lemma 15.6.** *For each positive integers  $k, v$ , there exists a first-order formula  $\alpha_k^v(g; z_1, \dots, z_k)$  of length  $O(k + \log v)$  such that for each group  $G$  of size at most  $v$ ,  $G \models \alpha_k^v(g; z_1, \dots, z_k)$  if and only if  $g \in \langle z_1, \dots, z_k \rangle$ .*

Given a group  $G$  of size at most  $v$ , we write  $L_k^v(\bar{z}) = \{y \in G : G \models \alpha_k^v(y; \bar{z})\}$  in case this is a subgroup.

Every finite group has a generating set of logarithmic size. So a group  $G$  of size at most  $v$  is simple iff

$$G \models \forall z_1, \dots, z_k [L_k^v(\bar{z}) \triangleleft G \rightarrow (L_k^v(\bar{z}) = \{e\} \vee L_k^v(\bar{z}) = G)],$$

where  $k = \log v$ .

One can use these facts to give a new type of first-order description of finite simple groups in logarithmic length. First one says what the size of the groups is, and that it is simple. A finite simple group is determined by its size, with the exception of

- $\text{PSL}_3(4)$  which has the same size as  $\text{Alt}_8$  without being isomorphic to it, and
- the groups  $B_n = P\Omega_{2m+1}(q)$  and  $C_m = \text{PSp}_{2m}(q)$ ,  $q$  an odd prime power,  $m > 2$ , which have the same size  $\frac{1}{2}q^{m^2} \prod_{i=1}^m (q^{2i} - 1)$  without being isomorphic.

(See <http://mathoverflow.net/questions/107620/non-isomorphic-finite-simple-groups-for-background>.) The exceptional cases above can be distinguished by the fact that the nonisomorphic groups of the same size have different numbers of conjugacy classes of involutions, and that the number of these conjugacy classes is logarithmic in the size. Firstly, in  $\mathrm{PSL}_3(4)$  all involutions are conjugate, while in  $A_8$  there are two conjugacy classes, namely  $(12)(34)$  and  $(12)(34)(56)(78)$ . Next, in  $B_m$  there are  $m$  classes, in  $C_m$  for  $m$  odd there are  $(m+1)/2$  classes and for  $m$  even there are  $m/2 + 1$  classes. For the latter, see [18, Table 4.5.1, p. 172]. To read this table, note that classes in the simple group are the coset '1', diagonal involutions (outer automorphisms of the simple group) are labelled 'd'. The notation  $1/d$  [condition] means 1 if condition holds,  $d$  if condition does not hold. (Thanks to David Craven for pointing out the reference and explaining this.)

We note that [27, Lemma 2.5] shows that the number of involutions of  $B_m, C_m$  also differs for  $m > 2$ . This could also be used. (Thanks to Csaba Schneider for this reference.)

#### 16. MELNIKOV AND NIES: A COMPUTABLE COMPACT ABELIAN GROUP SUCH THAT THE HAAR MEASURE IS NOT COMPUTABLE

Melnikov and Nies worked at the Research Centre Coromandel in June. Recall a computable topological space  $X$  is given by a sequence of basis sets  $\langle B_n \rangle_{n \in \mathbb{N}}$  such that for every two such sets  $B_i, B_k$  we can uniformly represent  $B_i \cap B_k$  as an effective union of basic sets. Each computable metric space is also a computable topological space with the basis given by the  $B_\delta(p)$  for  $\delta \in \mathbb{Q}^+$  and  $p$  a special point. We say that a Borel measure  $\mu$  on  $X$  is computable if  $\mu(B_i)$  is uniformly left-c.e. in  $i$  (if boundaries of open sets are null we could as well require that it is uniformly computable).

A *computable topological group* is a group  $G$  that is also a computable topological space, in such a way that the group operations are effectively continuous.

Recall that every separable compact group has a unique translation invariant probability measure, called the Haar measure.

**Theorem 16.1.** *There is a computable compact abelian group such that the Haar measure is not computable.*

*Proof.* Let  $K$  denote the halting problem with effective enumeration  $\langle K_s \rangle$ ; we may assume that  $K_2 = \emptyset$ . We first give uniformly in  $e$  a presentation of a discrete cyclic group  $G_e$  such that the Haar measure on  $G_e$  is not uniformly computable.

For a real  $\theta$  let  $[\theta] = e^{2\pi i \theta}$ . The distance between two points on the circle is the usual shortest arc length.

We define a computable real  $v = v_e$  uniformly in  $e$ ;  $[v_e]$  will be a generator of  $G_e$  seen as a subgroup of the circle group. At stage  $s$ , if  $e \notin K_s$ , define  $v_s = \frac{1}{2} + 2^{-s}$ . If  $e \in K_s \setminus K_{s-1}$  define  $v_t = v_{s-1}$  for all  $t \geq s$ .

The special points of  $G_e$  are the uniformly computable reals given by the Cauchy name  $\langle i v_{s+i} \rangle_{s \in \mathbb{N}}$ . If  $e \notin K$  then  $G_e = \{[0], [1/2]\}$ ; if  $e \in K$  then  $|G_e| \geq 8$ .

The discrete topology on  $G_e$  is uniformly computable: as an effective basis take the sets  $G_e \cap B_\delta([iv^e])$  for  $\delta \in \mathbb{Q} \cap (0, 1/2]$ . Let  $\mu_e$  be Haar measure on  $G_e$  with the discrete topology. Clearly by the translation invariance of  $\mu_e$  we have  $e \notin K \leftrightarrow \mu_e(B_{1/8}(1)) > 1/4$ . So  $\mu_e$  is not uniformly computable.

Now let  $G = \prod_e G_e$  topologized with the product topology which is compact and effective with the usual product basis. Let  $p_e: G \rightarrow G_e$  be the projection onto  $G_e$  which is computable uniformly in  $e$ . If the Haar measure on  $G$  is computable then the image measure  $p_e(\mu)$  on  $G_e$  is uniformly computable. However,  $\mu_e = p_e(\mu)$  by uniqueness of Haar measure, contradiction.  $\square$

## 17. FOUCHE AND NIES: COMPUTABLE PROFINITE GROUPS

Willem Fouché and Nies went on a 1-week retreat near Port Elizabeth, South Africa, and before and after worked at Unisa Pretoria. As one topic they studied randomness in computable profinite groups.

**17.1. Background on profinite groups.** A separable compact group  $G$  is called *profinite* if  $G$  is the inverse limit

$$G = \varprojlim_n \langle G_n, p_n \rangle_{n \in \mathbb{N}}$$

of a system of discrete finite groups

$$\rightarrow_{p_n} G_n \rightarrow_{p_{n-1}} G_{n-1} \rightarrow \dots \rightarrow_{p_2} G_2 \rightarrow_{p_1} G_1.$$

The inverse limit is determined up to isomorphism by the universal property formulated in terms of category theory. For a concrete instantiation, it can be seen as a closed subgroup  $U$  of the direct product  $\prod_n G_n$  consisting of the functions  $\alpha$  such that  $p_n(\alpha(n+1)) = \alpha(n)$  for each  $n > 0$ .

We may assume that the maps  $p_n$  are onto after replacing  $G_n$  by its subgroup of elements such that all the iterated pre-images under the maps  $p_i$  are defined. This corresponds to pruning a tree by removing dead ends.

**Remark 17.1** (Haar measure). Given  $G$  as an inverse limit of an onto system, the Haar probability measure  $\mu$  can be concretely defined as follows. Let  $q_n: G \rightarrow G_n$  be the natural projection. A clopen set  $C$  of  $G$  has the form  $C = q_n^{-1}(F)$  for a finite set  $F \subseteq G_n$ . By definition  $\mu$  is translation invariant, so  $\mu(C) = |F|/|G_n|$ . As the clopen sets form a basis this determines the measure on all the Borel sets of  $G$ .

*Completion.* The definition below is taken from [37, Section 3.2]. Let  $G$  be a group,  $\mathcal{V}$  a set of normal subgroups of finite index in  $G$  such that  $U, V \in \mathcal{V}$  implies that there is  $W \in \mathcal{V}$  with  $W \subseteq U \cap V$ . We can turn  $G$  into a topological group by declaring  $\mathcal{V}$  a basis of neighbourhoods (nbhds) of the identity. In other words,  $M \subseteq G$  is open if for each  $x \in M$  there is  $U \in \mathcal{V}$  such that  $xU \subseteq M$ .

**Definition 17.2.** The completion of  $G$  with respect to  $\mathcal{V}$  is the inverse limit

$$G_{\mathcal{V}} = \varprojlim_{U \in \mathcal{V}} G/U,$$

where  $\mathcal{V}$  is ordered under inclusion and the inverse system is equipped with the natural maps: for  $U \subseteq V$ , the map  $p_{U,V}: G/U \rightarrow G/V$  is given by  $gU \mapsto gV$ .

The inverse limit can be seen as a closed subgroup of the direct product  $\prod_{U \in \mathcal{V}} G/U$  (where each group  $G/U$  carries the discrete topology), consisting of the functions  $\alpha$  such that  $p_{U,V}(\alpha(gU)) = gV$  for each  $g$ . Note that the map  $g \mapsto (gU)_{U \in \mathcal{V}}$  is a continuous homomorphism  $G \rightarrow G_{\mathcal{V}}$  with dense image; it is injective iff  $\bigcap \mathcal{V} = \{1\}$ .

If the set  $\mathcal{V}$  is understood from the context, we will usually write  $\widehat{G}$  instead of  $G_{\mathcal{V}}$ .

*Free profinite groups.*

**Definition 17.3.** Let  $\widehat{F}_k$  be the free profinite group in  $k$  generators  $x_0, \dots, x_{k-1}$  ( $k < \omega$ ).

Clearly,  $\widehat{F}_k$  is the profinite completion of the abstract free group on  $k$  generators with respect to the system of all subgroups of finite index. Any topologically finitely generated profinite group can be written in the form

$$\widehat{F}_k/R$$

for some  $k$  and a closed normal subgroup  $R$  of  $\widehat{F}_k$ .

**Definition 17.4.** Let  $\widehat{F}_{\omega}$  be the free profinite group on a sequence of generators  $x_0, x_1, x_2 \dots$  converging to 1 [37, Thm. 3.3.16].

Thus,  $\widehat{F}_{\omega}$  is the completion in the sense of the previous subsection of the free group  $F_{\omega}$  on generators  $x_0, x_1, \dots$  with respect to the system of normal subgroups of finite index that contain almost all the  $x_i$ . Any profinite group  $G$  has a generating sequence  $\langle g_i \rangle_{i \in \mathbb{N}}$  converging to 1. This is easy to see using coset representatives for a descending sequence of open normal subgroups that form a fundamental system of nbhds of  $1_G$ . (Also see [37, Prop. 2.4.4 and 2.6.1].) By the universal property of the completion, the map from the abstract free group induced by  $x_i \rightarrow g_i$  extends to a continuous epimorphism  $\widehat{F}_{\omega} \rightarrow G$ . So  $G$  can be written in the form

$$\widehat{F}_k/R$$

where  $R$  is a closed normal subgroup of  $\widehat{F}_k$ .

*“Almost everywhere” theorems in profinite groups.*

**Theorem 17.5** (Jarden; see [15], 18.5.6). *Let  $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  be the absolute Galois group of  $\mathbb{Q}$ . For almost all tuples  $\sigma = (\sigma_1, \dots, \sigma_e) \in G^e$ , the closed subgroup of  $G$  topologically generated by  $\sigma$ , is a free profinite group of rank  $e$ .*

A group  $G$  is called *small* if it has only finitely many subgroups of each index. Each small residually finite (r.f.) group is *hopfian*, namely, every epimorphism  $\alpha: G \rightarrow G$  is an isomorphism. (Proof: let  $V_n$  be the intersection of subgroups of index  $\leq n$ , and check that  $\alpha(V_n) = V_n$  for each  $n$ .) If  $g \in \ker \alpha$  and  $g \neq 1$  then  $g \notin V_n$  for some  $n$ , so  $\alpha(g) \neq 1$  as well.)

Every f.g. profinite group is small and r.f., and hence hopfian. It follows that  $\sigma$  above actually freely topologically generates  $G$ .



A field  $L$  is PAC (pseudo-algebraically closed) if every (irreducible) variety over  $L$  has a point in  $L$ . Besides algebraically closed fields, examples of PAC fields are the algebraic extensions  $L$  of  $\mathbb{F}_q$  with  $|L : \mathbb{F}_q| = \omega$ . See [15] for background. A field  $L$  is  $\omega$ -free if  $\text{Gal}(L)$  is topologically isomorphic to  $\widehat{F}_\omega$ .

**Theorem 17.6** (Jarden, see Thms 18.6.1 and 27.4.8 in [15]). *Let  $G = \text{Gal}(\mathbb{Q})$  be the absolute Galois group of  $\mathbb{Q}$ . For  $\sigma = (\sigma_1, \dots, \sigma_e) \in G^e$  let  $L_\sigma = \mathbb{Q}[\sigma]$  denote the maximal Galois extension of  $\mathbb{Q}$  contained in the fixed field of  $\sigma$ ; equivalently,  $L_\sigma$  is the fixed field of the normal closure of  $\sigma$ .*

*For almost all tuples  $\sigma$ ,  $L_\sigma$  is PAC and  $\omega$ -free.*

Jarden and Lubotzky [25] study a related setting, namely  $G = \widehat{F}_n$ .

**Theorem 17.7** (Jarden and Lubotzky, Thm. 1.4 in [25]). *Let  $G = \widehat{F}_n$  for finite  $n \geq 2$ . For almost all tuples  $\sigma = (\sigma_1, \dots, \sigma_e) \in G^e$ , the closed normal subgroup they topologically generate either has finite index or is a free profinite group of rank  $\omega$ . The second case holds for all  $\sigma$  if  $e < n$ , for almost all  $\sigma$  if  $e = n$ , and for a set of  $\sigma$  with positive measure if  $e > n$ .*

**17.2. The algorithmic theory.** This section has benefitted from discussions with A. Melnikov.

*Effectiveness conditions on profinite groups.*

**Definition 17.8** (Smith [41]).

- (i) A profinite group  $G$  is called *co-r.e.* if it is the inverse limit of a computable inverse system  $\langle G_n, p_n \rangle$  of finite groups (i.e. the groups  $G_n$  and the maps  $p_n$  between them are uniformly computable). Equivalently, the subgroup  $U$  above is a  $\Pi_1^0$  subclass of  $\prod_n G_n$ .
- (ii)  $G$  is called *computable* if, in addition, the maps  $p_n$  can be chosen onto. In other words, the set of extendible nodes in the tree corresponding to  $U$  is computable.

*Absolute Galois groups.* Let  $K$  be a computable field. Then the algebraic closure  $\overline{K}$  has a computable presentation. ( $\overline{\mathbb{Q}}$  has a unique one, i.e. is autostable, by a result of Ershov.)

Suppose in addition that  $K$  has a splitting algorithm (for polynomials in one variable), i.e. one can decide whether a polynomial is irreducible. An example of such a field is  $\mathbb{Q}$ . Then  $\overline{K}$  has a computable presentation so that the  $K$  viewed as a subset of  $\overline{K}$  is decidable [35, Lemma 6].

Also, the absolute Galois group of  $K$  is computable. To show this, intuitively, one builds a computable chain  $K = L_0 \leq L_1 \leq \dots$  of finite Galois extensions of  $K$  with union  $\overline{K}$ . The computable inverse system is given by the groups  $G_n = \text{Gal}(L_n/K)$  where the projection  $p_n : G_{n+1} \rightarrow G_n$  is given by restricting  $\phi \in \text{Gal}(L_{n+1}/K)$  to  $L_n$ .

*Computable profinite groups that are completions.* Suppose  $G$  is a computable group, and the class  $\mathcal{V}$  in Definition 17.2 is uniformly computable in that there is a uniformly computable sequence  $\langle R_n \rangle$  such that  $\mathcal{V} = \{R_n : n \in \mathbb{N}\}$ . Suppose further that  $W$  above can be obtained effectively from  $U, V$ . Then there is a uniformly computable descending subsystem  $\langle T_k \rangle$  of  $\langle R_n \rangle$



such that  $\forall n \exists k T_k \leq R_n$ . Since we can effectively find coset representatives of  $T_n$  in  $G$ , the inverse system  $\langle G/T_n \rangle$  with the natural projections  $T_{n+1}a \rightarrow T_na$  is computable. So  $G_\gamma$  is computable.

The criterion above is satisfied by  $F_k$  and  $F_\omega$  with the systems of normal subgroups introduced above. Thus their completions  $\widehat{F}_k$  and  $\widehat{F}_\omega$  are computable profinite groups.

**Lemma 17.9.** *Let  $G$  be  $k$ -generated ( $k \leq \omega$ ). Then  $G$  is computable [co-r.e.] iff  $G = \widehat{F}_k/N$  for some computable normal subgroup  $N$  ( $\Pi_1^0$   $N$ ).*

*Computability of Haar measure.* We use the notion of a computable probability space by Hoyrup and Rojas [23].

**Lemma 17.10.** *Let  $G$  be computable profinite group. Then  $\mu_G$ , the Haar probability measure on  $G$ , is computable.*

*Proof.* The inverse system  $\langle G_n, p_n \rangle$  is computable. So for a clopen set  $C = q_n^{-1}(F)$  as in Remark 17.1, given by the parameters  $n$  and  $F$ , we can compute the measure. This suffices.  $\square$

**Remark 17.11.** Here is a more concrete description of the Haar measure. As before  $q_n: G \rightarrow G_n$  is the natural projection. We also assume that  $G_1$  is trivial. We write  $V_n = \ker q_n$ . For each  $n$  we can effectively determine  $k_n = |V_n : V_{n+1}|$  and a sequence  $\langle g_i^{(n)} \rangle_{i < k_n}$  of coset representatives for  $V_{n+1}$  in  $V_n$  such that  $g_0^{(n)} = 1$ .

Let  $T$  be the tree of strings  $\sigma \in \omega^{<\omega}$  such that  $\sigma(i) < k_i$  for each  $i < |\sigma|$ . For  $|\sigma| = n$  we have a coset of  $V_n$  in  $G$

$$C_\sigma = g_{\sigma(0)}^{(0)} g_{\sigma(1)}^{(1)} \cdots g_{\sigma(n-1)}^{(n-1)} V_n.$$

The clopen sets  $C_\sigma$  form a basis for  $G$ . In this way  $G$  is naturally homeomorphic to  $[T]$  where the identity element corresponds to  $0^\omega$ . The Haar measure is the usual uniform measure on  $[T]$ .

*Randomness notions defined via algorithmic tests.* Let  $G$  be a computable profinite group. Given that the Haar measure  $\mu$  on  $G$  is computable, the usual randomness notions defined via algorithmic tests, or effectively descriptive set theory tests, can be applied. The usual question is: how strong a randomness notion on a group element  $g$  suffices for an “almost everywhere” properties to hold for  $g$ ?

A point in a computable measure space is Kurtz random (or weakly random) if it is in no  $\Pi_1^0$  null class. For Jarden’s Thm. 17.5, and at least the first part of his Thm. 17.6, this rather weak randomness notion is sufficient. If the underlying topological space is effectively homeomorphic to Cantor space, then any weakly 1-generic point (i.e., in every dense  $\Sigma_1^0$  set) is Kurtz random. As this applies to the setting of profinite groups at hand, the points for which Jarden’s results hold are also comeager.

**Theorem 17.12** (effective form of Jarden’s Thm. 17.5 for  $\mathbb{Q}$ ). *Let  $G = \text{Gal}(\mathbb{Q})$  be the absolute Galois group of  $\mathbb{Q}$ . Let  $\sigma = (\sigma_1, \dots, \sigma_e) \in G^e$  be Kurtz random. The closed subgroup generated by  $\sigma$  is a free profinite group of rank  $e$  (freely generated by  $\sigma$ ).*

Here is a sketch why this is true. (For a full proof, thorough understanding of Jarden's result would be needed, which is hard work because of the long chain of dependencies and heavy notation leading up to [15, 18.5.6].) All item numbers refer to [15].

Two extensions  $L_1, L_2$  of a common field  $K$  (tacitly assumed to be contained in a common field) are called *linearly disjoint* if whenever a tuple from  $L_1$  is linearly independent over  $K$ , it remains linearly independent over  $L_2$ . By Lemma 2.5.1. this is symmetric.

A sequence of extensions  $L_1, L_2, \dots$  is linearly disjoint if  $L_{j+1}$  is l.d. from the compositum  $L_1 \dots L_j$  for each  $j$ . Given  $k$ , Cor. 16.2.7. builds such a sequence of Galois extensions for  $K = \mathbb{Q}$  such that for each  $n$  we have  $\text{Gal}(L_n/\mathbb{Q}) \cong S_k$  via some isomorphism  $\rho_n$ . The sequence of fields  $\langle L_n \rangle$  is uniformly computable, as can be derived from the proof (hopefully).

By 18.5.1. the linear disjointness implies that the absolute Galois groups  $\text{Gal}(L_n) \leq \text{Gal}(\mathbb{Q})$  are  $\mu$ -independent; recall that  $\mu$  is the Haar measure on  $G = \text{Gal}(\mathbb{Q})$ . More generally, by 18.5.2, for  $e \geq 1$ , if for each  $n$  one picks a coset  $C_n$  of  $\text{Gal}(L_n)^e$  in  $G^e$ , the  $C_n$  are  $\mu^e$ -independent.

Now to conclude the argument, we want to show that each finite group  $R$  generated by  $e$  elements is a quotient of the closed subgroup  $\langle \sigma \rangle \leq G$  generated by  $\sigma$ , as this suffices to show freeness. Embed  $R$  into  $S_k$  for  $k$  sufficiently large, and let  $\pi_1, \dots, \pi_e$  be the images of the generators of  $R$  under this embedding.

For each  $n$  we have a natural onto homomorphism  $G \rightarrow \text{Gal}(L_n/\mathbb{Q})$  given by restriction to  $L_n$  (note that  $L_n$ , being a normal extension of  $\mathbb{Q}$ , is preserved under automorphisms of  $\overline{\mathbb{Q}}$ ). So we can effectively pick a coset  $C_n$  of  $\text{Gal}(L_n)^e$  in  $G^e$  that maps to  $\langle \pi_1, \dots, \pi_e \rangle$ . Since the  $L_n$  are independent, these cosets are independent, and each has measure  $1/(k!)^e$ . Hence, by Borel-Cantelli their union has measure 1. The union is  $\Sigma_1^0$  and hence contains the Kurtz random  $\sigma$ . This shows that  $R$  is a quotient of  $\langle \sigma \rangle$  as required.

**Theorem 17.13** (effective form of the first part of Jarden's Thm. 17.6 for  $\mathbb{Q}$ ). *In the setting of Thm. 17.6, recall that for an automorphism  $\sigma \in \text{Gal}(\mathbb{Q})$ ,  $L_\sigma$  is the fixed field of the normal closure of  $\sigma$ . If  $\sigma$  is Kurtz random, then  $L_\sigma$  is PAC.*

*Proof.* We first show that  $L_\sigma$  is uniformly computable from (a code for)  $\sigma$ . For  $x \in \overline{\mathbb{Q}}$  to be in  $L_\sigma$ , it suffices that each conjugate  $\tau^{-1}\sigma\tau$  fixes  $x$ , or equivalently  $\sigma(y) = y$  for each  $y$  in the orbit of  $x$  under the action of  $\text{Gal}(\mathbb{Q})$ . This orbit consists of all the conjugates of  $x$ , and can be computed from  $x$ .

By Jarden's theorem and the fact that a Kurtz random is in every  $\Pi_2^0$  conull set, it now suffices to show that the PAC subfields  $K$  of  $\overline{\mathbb{Q}}$  form a  $\Pi_2^0$  class.

Recall that for a unital ring  $R$ , a nonconstant polynomial in  $R(X_1, \dots, X_n)$  is called irreducible if it cannot be written as a product for two nonconstant polynomials. For a field  $K$ , a polynomial in  $K[X_1, \dots, X_n]$  is called *absolutely irreducible* if it is irreducible in  $\overline{K}[X_1, \dots, X_n]$ . We use some facts on PAC fields from [15, Section 11.3]. [15, Theorem 11.2.3] implies:

**Proposition 17.14.** *A field  $K$  is PAC if and only if for every absolutely irreducible polynomial  $f \in K[X, Y]$ , there is a point  $(a, b) \in K^2$  with  $f(a, b) = 0$ .*

This yields the required  $\Pi_2^0$  condition as soon as we can express using a  $\Pi_1^0$  condition on the coefficients of  $f$  that a polynomial  $f \in K[X, Y]$  is absolutely irreducible. But irreducibility of  $f$  in the polynomial ring  $R[X_1, \dots, X_n]$  is a  $\Pi_1^0$  condition on the coefficients of  $f$  for any computable ring  $R$ , as one sees directly by inspecting the definition.  $\square$

**Remark 17.15.** The conditions (1) on page 200 in [15, Section 11.3] yield a set of sentences in first-order logic expressing that a field is PAC.  $S_K(2, d)$  denotes the set of polynomials  $f \in K(X, Y)$  of degree  $< d$  in both  $X$  and  $Y$ . They say that for each irreducible  $h \in \mathbb{Q}(T)$ , some  $\Pi_1^0$  condition holds (for each triple of polynomials  $g_1, g_2, g_3$  of bounded degree, something not involving quantifiers fails). It is decidable whether  $h$  is irreducible as  $\mathbb{Q}$  has a splitting algorithm, so we can also get a co-r.e. condition on coefficients in this way.

*Potential generalisation to Hilbertian fields.* A field  $K$  is Hilbertian if every finite set of irreducible polynomials in a finite number of variables and having coefficients in  $K$  admit a common specialization of a proper subset of the variables to field elements such that all the polynomials remain irreducible (Wikipedia). Hilbert showed that  $\mathbb{Q}$  has this property (Hilbert's irreducibility theorem). All the classic a.e. theorems from [15] mentioned above are stated for any countable Hilbertian field, rather than just for  $\mathbb{Q}$ . If  $K$  is computable and has the effective splitting property, then one can expect that the effective versions hold as well.

## 18. RUTE: ON THE COMPUTABILITY OF COMPACT GROUPS

This note covers basic theorems about the computability of Haar measures and profinite groups. The results are due to Jason Rute and were proved after discussions with Nies and Melnikov.

While we could work in the more general context of computable topological spaces, we will only focus here on computable metric spaces (also known as computably presented Polish spaces), since they are well understood.

Recall that a *computable metric space*  $\mathbb{X}$  is a complete separable metric space  $(X, d)$  along with a dense sequence of points  $(a_i)$  such that the map  $i, j \mapsto d(a_i, a_j)$  is computable. We say  $\mathbb{X}$  is *effectively compact* if one can enumerate all  $\Sigma_1^0$  sets which cover  $\mathbb{X}$ . It is easy to see that Cantor space is effectively compact. We will need the following well-known properties about effectively compact spaces.

**Proposition 18.1.** *Let  $\mathbb{X}$  be a computable metric space along with a computable sequence  $A_n$  where  $A_n$  is a list of points  $(a_1^n, \dots, a_k^n)$  such that every point in  $\mathbb{X}$  is within distance  $2^{-n}$  of some  $a_i^n$ . Then  $\mathbb{X}$  is effectively compact.*

*Proof.* Using the double sequence  $(a_i^n)$  we can construct a computable onto map  $f: 2^{\mathbb{N}} \rightarrow \mathbb{X}$ . (The details are routine but a bit technical. A similar construction can be found in Simpson [40, IV.1].) Now, we want to enumerate all effectively open covers of  $\mathbb{X}$ . That is the same as enumerating all empty

$\Pi_1^0$  subsets of  $\mathbb{X}$ . Consider a  $\Pi_1^0$  set  $P \subseteq \mathbb{X}$ . The set  $f^{-1}(P)$  is  $\Pi_1^0$  subset of  $2^{\mathbb{N}}$ , and it is empty iff  $P$  is empty. Since  $2^{\mathbb{N}}$  is effectively compact we will enumerate  $f^{-1}(P)$  eventually if it is empty, and then we can use that to enumerate  $P$ .  $\square$

**Proposition 18.2.** *If  $\mathbb{X}$  is an effectively compact computable metric space and  $\{a\} \subseteq \mathbb{X}$  is a  $\Pi_1^0$  singleton set, then  $a$  is computable. If  $f: \mathbb{X} \rightarrow \mathbb{X}$  is a function whose graph  $f \subseteq \mathbb{X} \times \mathbb{X}$  is  $\Pi_1^0$ , then  $f$  is computable.*

*Proof.* Let  $U$  be the complement of  $\{a\}$ . Compute  $a$  by enumerating covers of the space of the form  $U \cup B$  where  $B$  is a basic open ball of small radius. Similarly, use this method to compute  $f(x)$  from  $x$ .  $\square$

**Definition 18.3.** A *computable topological Polish group* to be a computable metric space  $G$  with a computable group operation and a computable inverse operation.<sup>2</sup>

The computable analogue of a compact group is a computable Polish group which is effectively compact.

**Fact 18.4.** *If  $G$  is an effectively compact computable metric space with a computable group operation, then the inverse operation is also computable, and therefore  $G$  is a computable Polish group.*

*Proof.* Notice that the graph of the inverse function  $\{(g, g^{-1}) \mid g \in G\}$  is a  $\Pi_1^0$  set. So the inverse map is computable by Proposition 18.2.  $\square$

If  $\mathbb{X}$  is a computable metric space, then the space of Borel probability measures on  $\mathbb{X}$  is also a computable metric space. In particular, a Borel probability measure  $\mu$  is computable if and only if the map  $f \mapsto \int f d\mu$  is a computable map for all bounded computable functions  $f: \mathbb{X} \rightarrow \mathbb{R}$ . If  $\mathbb{X}$  is effectively compact, then so is the space of Borel probability measures on  $\mathbb{X}$ . For more on the computability of Borel probability measures, see Hoyrup and Rojas [22] or Bienvenu, Gacs, Hoyrup, Rojas, and Shen [2].

**Proposition 18.5.** *Let  $G$  be an effectively compact computable Polish group. Then the left and right Haar probability measures are computable.*

*Proof.* The set of, say, left Haar probability measures is a  $\Pi_1^0$  singleton set in the effectively compact space of Borel probability measures on  $\mathbb{X}$ . By Proposition 18.2 the left Haar measure is computable.  $\square$

<sup>2</sup>One may object to this definition of “computable Polish group” since in the literature a Polish space is only defined as a completely metrizable space. The choice of metric does not matter. In a similar way, we could develop an equivalence relation on presentations of computable metric spaces. We say that two presentations of a computable metric space are equivalent if the identity and its inverse are computable. For example,  $\mathbb{R}^2$  with the Euclidean ( $\ell_2$ ) metric and the  $\ell_\infty$  metric are equivalent with any natural choice of dense set. Then we can define a *computable Polish space* as the set of equivalence classes of computable metric spaces. Similarly, we can use this idea to give a slightly more natural definition of *computable Polish group*, again as equivalence classes. The downside of this approach is that we need to constantly show that the properties we are interested in are preserved by this equivalence relation. For example, if two presentations of a space  $\mathbb{X}$  are equivalent, and one presentation is effectively compact, then so is the other presentation. Also, if two presentations of  $\mathbb{X}$  are equivalent, then so are the various corresponding presentations of the space of Borel probability measures on  $\mathbb{X}$ .

**Theorem 18.6.** *Let  $G$  be a compact computable Polish group for which the (left) Haar probability measure is computable. Then  $G$  is effectively compact.*

*Proof.* We re-metrize the space  $G$  by replacing  $d(x, y)$  with the average of  $d(gx, gy)$  where the average (the integral) is taken in the Haar measure as  $g$  varies across the group. This new metric is computable since  $d(x, y)$  is a bounded computable function. (The metric is bounded by the compactness of  $G$ .) Now one has a computable  $G$ -invariant distance which is equivalent to the original distance.

Now, to show that  $G$  is effectively compact in this new metric, it is enough for each rational  $k$ , to effectively find a finite set of points  $a_0^k, \dots, a_{n-1}^k$  for which every point in  $G$  is within distance  $2^{-k}$  of one of these points. Fix  $k$ . Using our Haar measure find the measure of a ball of radius  $2^{-(k+1)}$ . Call this measure  $\delta$ . (Since the new distance is  $G$ -invariant, all balls of the same radius have the same measure.) Using blind search find a collection of balls  $B_0, \dots, B_{n-1}$  of balls with radius  $2^{-(k+1)}$  whose union  $C = B_0 \cup \dots \cup B_{n-1}$  has measure  $> 1 - \delta$ . Now, consider any point  $x$  not in this union  $C$ . It has to be distance  $< 2^{-(k+1)}$  from the union. Otherwise, there would be a ball centered at  $x$  with radius  $2^{-(k+1)}$ , and hence measure  $\delta$ , which is disjoint from the union  $C$ . But the union  $C$  has measure  $> 1 - \delta$ , so this cannot happen. Therefore all points of  $G$  are within distance  $2^{-k}$  of the centers of  $B_0, \dots, B_{n-1}$ . This algorithm shows that the space is effectively compact in the new metric. To show it is effectively compact in the original metric, for any finite list of rational balls in original metric, convert it to a list of balls in the new metric. Now, if this list of balls covers the space  $G$ , by effective compactness, we will eventually find this out.  $\square$

**Example 18.7.** *There is a computable group  $G$  isomorphic to a product of finite cyclic groups  $\Pi_n G_n$  which is compact but for which the Haar measure is noncomputable.*

*Proof.* Let  $h(n)$  be the characteristic function of the Halting set. Then we will let  $G = \prod_n \mathbb{Z}_{2^{h(n)}}$  with the ultrametric  $\rho(f, g) = \inf\{2^n \mid f(n) \neq g(n)\}$ . This is a computable metric space (but it is not effectively compact). It is also a computable Polish group. The Haar measure of any cylinder set of length  $n$  is equal to  $\prod_{k < n} 2^{-h(k)}$ . If we could compute the Haar measure, then we could compute  $h(n)$ .  $\square$

As Section 17 in this year's Logic Blog mentioned, a profinite group is an inverse limit of finite groups. So there exists a descending chain of normal clopen subgroups  $N_s \triangleleft G$  which converges to the identity. Then  $G$  is the inverse limit of  $G/N_s$ . A  $G$  is computably profinite.

**Theorem 18.8.** *Let  $G$  be a profinite effectively compact computable Polish group. Then we can compute a sequence of finite groups  $G_s$  such that  $G$  is the inverse limit  $\varprojlim G_s$  and the corresponding homomorphism  $h_s: G \rightarrow G_s$  is computable.*

*Proof.* Since  $G$  is profinite, we need to find a descending chain of normal clopen subgroups  $N_s \triangleleft G$ . Since  $G$  is effectively compact, we can enumerate all clopen sets  $A$  by finding disjoint covers made up of finitely many open balls  $B_1, \dots, B_n, C_1, \dots, C_m$  where  $B_i$  and  $C_j$  are disjoint. We can then use

this to enumerate all normal clopen subgroups as follows. Since each clopen set  $A$  is both effectively open and closed, the property

$$\forall g \in G \quad gAg^{-1} \subseteq A$$

is  $\Pi_1^0$  (if the property fails, then search for some  $g \in G$  and some  $a \in A$  such that  $gag^{-1}$  is outside of  $A$ ) and  $\Sigma_1^0$  (if the property holds, then wait for an enumeration of balls which cover  $gAg^{-1}$  and which are disjoint from a cover of the complement of  $A$ ). Therefore, we can enumerate all clopen normal subgroups  $N \triangleleft G$ .

Let  $N_s$  be the intersection of all clopen normal subgroups enumerated at stage  $s$  of the construction (where  $N_0 = G$ ). This is also a clopen normal subgroup. Now enumerate all cosets  $gN_s$ . (These can be enumerated since each coset  $gN_s$  is also clopen. Also we know when we have enumerated them all since they form an open cover of an effectively compact space.) From this we can compute  $G/N_s$  along with the corresponding homomorphism. (If  $G$  is finite, then at some stage,  $G/N_s$  is isomorphic to  $G$ .)  $\square$

## Part 7. Metric spaces and descriptive set theory

### 19. NIES AND WEISS:

#### COMPLEXITY OF TOPOLOGICAL ISOMORPHISM FOR SUBSHIFTS

Let  $\Sigma$  be a finite alphabet. A *subshift* is a closed subset  $X \subseteq \Sigma^{\mathbb{Z}}$  which is invariant under the shift  $\sigma$ . We consider the complexity of the isomorphism relation  $(X, \sigma_X) \cong (Y, \sigma_Y)$  where  $\Sigma, \Delta$  are finite alphabets and  $X \subseteq \Sigma^{\mathbb{Z}}$ ,  $Y \subseteq \Delta^{\mathbb{Z}}$  are subshifts. To be isomorphic means that there is a continuous bijection  $\theta : X \rightarrow Y$  such that  $\theta(\sigma_X(z)) = \sigma_Y(\theta(z))$  for each  $z \in X$ . Note that  $\theta$  is given by the clopen sets  $\theta^{-1}(\{Z : Z(0) = b\})$  for  $b \in \Delta$ , which are of the form  $\bigcup_{i < k} [\alpha_i]$  where  $\alpha_i : [-N, N] \rightarrow \Sigma$  (such a collection of clopen sets is called a block code). So isomorphism is a countable Borel equivalence relation.

J. Clemens (Israel J. of Maths, 2009) proved that isomorphism is in fact a  $\leq_B$ -complete countable Borel equivalence relation.

A subshift is *minimal* if every orbit of an element is dense; equivalently, every possible pattern (i.e. subword of a fixed length of an element of the subshift) occurs in a large enough section of every element of the subshift. By compactness, the length of this section only depends on the pattern. As a consequence, minimality is a Borel property of subshifts. Also, it is sufficient to require the property that patterns re-occur within a distance only dependent on the pattern for one word with dense orbit.

Clemens asked in the paper and in a 2014 talk (available on youtube) the following question:

**Question 19.1.** *How complex is the isomorphism relation between minimal subshifts?*

Gao, Jackson and Seward [17, Section 9.3] proved that  $E_0$  is Borel reducible to isomorphism of minimal subshifts.

*Proof.* Here is a sketch of a short proof of this fact.



The idea is to build a sequence of blocks  $A_n, B_n$  of length  $L_n = (66)^n$ . The construction is controlled by a fixed element  $x \in \{0, 1\}^{\mathbb{N}}$  with the  $n$ -stage blocks a function of  $x_i$  for  $1 \leq i \leq n$ . This sequence of blocks determines a subshift  $S_x$ : the allowed patterns of length  $L_n$  are the  $A_n$  and  $B_n$ .

The blocks  $A_{n+1}, B_{n+1}$  will be built out of the  $n$ -stage blocks in such a way that any bi-infinite sequence formed by concatenating these two blocks has a unique parsing into blocks of these two types. This parsing defines for each bi-infinite word  $\langle z(i) \rangle_{i \in \mathbb{Z}}$  a unique integer modulo  $L_n$  which indicates the position of  $z(0)$  in the block.

Recall that an odometer is a dynamical system that is an inverse limit of periodic rotations. The simplest example is the 2-adic integers with addition by 1. Since  $L_{n+1}$  is a multiple of  $L_n$ , the position of  $z(0)$  modulo  $L_{n+1}$  when reduced modulo  $L_n$  gives the position of  $z(0)$  in its “ $n$ -block”. This will yield a common odometer as a factor of all the minimal shifts.

Let  $A_0 = 0$  and  $B_0 = 1$ . We describe 4 recipes for concatenating  $A, B$ :

1.  $AB(A^4B^4)^8$
2.  $AB(A^8B^8)^4$
3.  $AB(A^{16}B^{16})^2$
4.  $ABA^{32}B^{32}$ .

Depending upon the value of  $x_n$  the  $A_{n+1}, B_{n+1}$  will be formed in two different ways. If  $x_{n+1} = 1$  one uses 1 and 2, otherwise one uses 3 and 4. Assuming that one can recognize A and B, the initial ABA in all recipes guarantees that the concatenations have a unique parsing.

The minimality is immediate since all four possibilities AA, AB, BA, BB occur.

Each specific minimal system has its own collection of the two types of blocks, where the nature of the blocks up to level  $n$  depend only on the first  $n$  bits of the control element from  $0, 1^{\mathbb{N}}$ . Clearly if  $x$  and  $y$  agree from some point on there is a finite block code that will map one shift to the other. If  $x$  and  $y$  differ infinitely often then no matter what the length of the code eventually it will pick up the pattern of repetitions which differ significantly in all 4 recipes.  $\square$

Simon Thomas [42] has given a Borel reduction of  $E_0$  to a special class of minimal subshifts, the Toeplitz subshifts. A Toeplitz word is a bi-infinite word  $W$  such that for  $n \in \mathbb{Z}$  there is a “local period”  $k \in \mathbb{Z}$  such that  $\forall i \in \mathbb{Z} [W(n) = W(n + ik)]$ . A subshift is Toeplitz if it contains a Toeplitz word with dense orbit. To see that this is minimal, suppose that  $w$  is a subword of  $W$ , and let  $r$  be the l.c.m. of the local periods of any symbol in  $w$ . Then  $\sigma^r(w)$  is also a subword of  $W$ , for any  $r \in \mathbb{Z}$ .

Not much beyond that is known so far on the complexity of conjugacy for minimal subshifts.

## Part 8. Higher computability theory/effective descriptive set theory

### 20. YU: $\Pi_1^1$ -HYPERARITHMETIC DETERMINACY

Input by Yu.

The following theorem was claimed in [21]: the hyperdegrees of a  $\Pi_1^1$  set with a perfect subset contain an upper cone.

**Theorem 20.1** (Harrington [21]). *Let  $A \subseteq 2^\omega$  is a  $\Pi_1^1$  set that contains a perfect subset. There is a real  $z \in 2^\omega$  so that for any real  $y \geq_h z$ , there is a real  $x \in A$  for which  $x \equiv_h y$ .*

The following proof is based on some communications with Leo Harrington. His original idea seem model theoretical. Here is a tree proof.

The following theorem is proved by Martin.

**Theorem 20.2** (Martin [28]). *If  $A$  is an uncountable  $\Delta_1^1$ -set, then for any real  $y \geq_h \mathcal{O}$ , there is a real  $x \in A$  for which  $x \equiv_h y$ .*

Fix an uncountable  $\Pi_1^1$  set  $A$  throughout in this section. Since  $A$  is  $\Pi_1^1$ , there is a recursive oracle functional  $\Phi$  so that

$$x \in A \Leftrightarrow \Phi^x \text{ codes a well ordering of } \omega.$$

In other words, the binary relation  $n \leq_x m$  if and only if  $\Phi^x(\langle n, m \rangle) = 1$  is a well ordering over  $\omega$ . We use  $n \in \text{Dom}(\Phi^x)$  to denote that there is some  $m$  so that  $\Phi^x(\langle n, m \rangle) = 1$  or  $\Phi^x(\langle m, n \rangle) = 1$ . For a finite binary string  $\sigma$ , we also use  $<_{\Phi^\sigma}$  to denote the finite linear order coded by  $\Phi^\sigma$ .

Let

$$\beta = \min\{\beta \mid |\{x \mid \Phi^x \text{ codes a well ordering of } \omega \text{ with order type } \beta\}| > \aleph_0\}.$$

Since  $A$  has a perfect subset, such  $\beta$  must exist.

We fix the  $\beta$  throughout.

We associate a tree  $T$  with  $A$  by defining  $(\sigma, \tau) \in T$  if and only if

- (1)  $\sigma \in 2^{<\omega}$  and;
- (2)  $\tau$  is finite order preserving function from  $\text{Dom}(\Phi^\sigma)$  to ordinals.

We always assume that  $|\text{Dom}(\Phi^\sigma)| = |\sigma|$ .

$(\sigma_0, \tau_0) \preceq (\sigma_1, \tau_1)$  if both  $\sigma_1$  and  $\tau_1$  extends  $\sigma_0$  and  $\tau_0$  respectively.  $(\sigma_0, \tau_0)$  is at the left of  $(\sigma_0, \tau_0)$  if

- (1) for some are  $m \leq \min\{|\sigma_0|, |\sigma_1|\}$ ,  $\sigma_0 \upharpoonright m = \sigma_1 \upharpoonright m$  but  $\sigma_0(m+1) < \sigma_1(m+1)$  or
- (2) for every  $\sigma_0 \upharpoonright \min\{|\sigma_0|, |\sigma_1|\} = \sigma_1 \upharpoonright \min\{|\sigma_0|, |\sigma_1|\}$  and for some  $k$ ,  $\tau_0(k) < \tau_1(k)$  but  $\tau_0(j) = \tau_1(j)$  for all  $j <_{\Phi^\sigma} k$ .

Then  $x \in A$  if and only if there is an  $f$  so that  $(x, f)$  is an infinite branch of  $T$ .

Let  $T^\beta$  be the tree  $T$  restricted to the ordinal  $\beta$ , i.e. the range of every  $\sigma$  is a subset  $\beta + 1$ . Obviously  $T^\beta \in L_{\omega_1^\beta}$ . Moreover, there are uncountable many infinite branches in  $T^\beta$  by the definition of  $\beta$ . Let

$$A_\beta = \{x \mid \Phi^x \text{ codes a well ordering of } \omega \text{ of order type } \leq \beta\}.$$

Then  $A_\beta$  is exactly the collection of reals  $x$  for which there is an  $f$  so that  $(x, f)$  is an infinite branch through  $T^\beta$ .

Obviously  $A_\beta$  is an uncountable Borel set containing a perfect subset.

Let  $\omega_1^\beta$  be the least admissible ordinal greater than  $\beta$ . Obviously  $T^\beta \in L_{\omega_1^\beta}$ .



**20.1. Case(1): There is a real  $z$  so that  $z \in L_{\omega_1^\beta}$  and  $\omega_1^z = \omega_1^\beta$ .** Then let  $B_\beta = \{x \mid \Phi^x \text{ codes a well ordering of order type } \beta\} \subseteq A_\beta$  be a  $\Delta_1^1(z)$ -set. Then for any real  $x \in B_\beta$ ,  $x \geq_h z$ . Relativizing the proof of Theorem 20.2 to  $z$ , we may have Theorem 20.1.

**20.2. Case(2): Otherwise.** Then for any real  $x \in A_\beta$ , if  $\Phi^x$  codes a well ordering of  $\beta$ , then  $x \notin L_{\omega_1^\beta}$ .

Fix a recursive enumeration of set theoretical  $\Sigma_0$ -formulas  $\{\varphi_i(u, v, \beta)\}_{i \in \omega}$  with  $\beta$  as a parameter. Then  $\omega_1^\beta$  is the least ordinal  $\gamma > \beta$  so that for any  $i$ ,

$$L_\gamma \models \forall u < \beta \exists v \varphi_i(u, v, \beta) \rightarrow \exists w \forall u < \beta \exists v \in L_w \varphi_i(u, v, \beta).$$

We also do a Cantor-Bendixon derivation to  $T^\beta$ . I.e.  $T_0^\beta = T^\beta$ ; and for any stage  $\gamma < \omega_1^\beta$  and  $(\sigma_1, \tau_1) \succ (\sigma_0, \tau_0) \in T_\gamma^\beta$ , if

- (1) either there exists an order preserving (in the  $<_{KB}$  sense) function  $f \in L_\beta$  so that  $f : T_1^\beta[(\sigma_1, \tau_1)] \rightarrow \beta$ ; or
- (2) there exists a real  $x \in L_\beta$  so that  $\{x\} = \{z \succ \sigma_1 \mid \exists f \succ \tau_1 \forall n (x \upharpoonright n, f \upharpoonright n) \in T_\gamma^\beta\}$ ,

then we let  $T_1^{\beta+1} = T_1^\beta \setminus [(\sigma_1, \tau_1)]$  and claim that  $(\sigma_1, \tau_1)$  is cut off from  $T_\gamma^\beta$  at stage  $\gamma$ .

If  $\gamma$  is a limit stage, then  $T_\gamma^\beta = \bigcap_{\gamma' < \gamma} T_{\gamma'}^\beta$ .

Let

$$T_{\omega_1^\beta}^\beta = \bigcap_{\gamma < \omega_1^\beta} T_\gamma^\beta.$$

Obviously  $T_{\omega_1^\beta}^\beta$  is not empty.

Let  $T^1 \subseteq 2^\omega \times \omega^{<\omega}$  be a recursive tree so that  $p[T^1] = \{x \mid \exists f(x, f) \in [T^1]\} = \{x \mid x \notin L_{\omega_1^x}\}$ .

Since  $A_\beta$  contains a perfect subset,  $p[T^1] \cap A_\beta \neq \emptyset$ .

**Lemma 20.3.** *If  $x \in p[T^1] \cap A_\beta$ , then  $x \notin L_{\omega_1^\beta}$  and  $\omega_1^x \geq \omega_1^\beta$ . Moreover, if  $\Phi^x$  codes a well ordering of order type less than  $\beta$ , then  $x \in L_{\omega_1^x}$  and  $\omega_1^x \leq \omega_1^\beta$ .*

*Proof.* Fix a real  $x \in A_\beta$ .

If  $\Phi^x$  codes a well ordering of order type  $\beta$ , then  $\omega_1^x \geq \omega_1^\beta$ . So  $x \notin L_{\omega_1^\beta}$ .

If  $\Phi^x$  codes a well ordering of order type  $\gamma$  less than  $\beta$ , then  $A_\gamma$  is a countable set which is  $\Delta_1^1(z)$  for any real  $z$  with  $\omega_1^z \geq \gamma$ . Then  $x \leq_h z$  for any real  $z$  with  $\omega_1^z \geq \omega_1^\gamma$ . But  $\omega_1^x \geq \omega_1^\gamma$ . So  $x \in L_{\omega_1^\gamma}$  and  $\omega_1^\gamma = \omega_1^x$ . Hence  $x \notin p[T^1]$ .  $\square$

So if  $x \in p[T^1] \cap A_\beta$ , then  $x >_h \mathcal{O}$ .

Let

$$T^2 = T^1 \otimes T^\beta = \{(\sigma_0, \sigma_1, \sigma_2) \mid (\sigma_0, \sigma_1) \in T^1 \wedge (\sigma_0, \sigma_2) \in T^\beta\}.$$

Obviously  $T^2 \in L_{\omega_1^\beta}$  and  $[T^2]$  is not empty. Let  $(x, f, h)$  be the leftmost infinite path through  $T^2$ . Then  $x \in p[T^1] \cap A_\beta$  and so by Lemma 20.3,  $x \in L_{\omega_1^{\beta+2}} \setminus L_{\omega_1^\beta}$ . In other words, there must be a master code in  $L_{\omega_1^{\beta+2}} \setminus L_{\omega_1^\beta}$ .

Fix a standard master code  $z_0 \in L_{\omega_1^\beta+2} \setminus L_{\omega_1^\beta}$ .

Now let  $y_0 >_h z_0$  be a real.

**Definition 20.4.** Given a tree  $S \subset 2^{<\omega} \times \alpha^{<\omega}$  where  $\alpha$  is an ordinal, a finite pair  $(\sigma, \tau) \in S$  is called a *splitting node* in  $S$  if for any  $i \leq 1$ , there is some  $\gamma_i$  so that  $(\sigma \smallfrown i, \tau \smallfrown \gamma_i) \in S$ .

**Definition 20.5.** Given an infinite path  $(x, f) \in [T_{\omega_1^\beta}^\beta]$ , a number  $n$  and an ordinal  $\gamma \leq \omega_1^\beta$ , we say that  $\gamma$  is *correct up to  $n$  respect to  $(x, f)$*  if for any  $i \leq n$ ,  $(x \smallfrown i, f \smallfrown i)$  is a splitting node in  $T_{\omega_1^\beta}^\beta$  if and only if  $(x \smallfrown i, f \smallfrown i)$  is a splitting node in  $T_\gamma^\beta$ .

The following lemma is clear.

**Lemma 20.6.** Suppose that  $(x, f) \in [T_{\omega_1^\beta}^\beta]$ ,  $n$  is a number and  $\gamma \leq \gamma' \leq \omega_1^\beta$ . If  $\gamma$  is correct up to  $n$  respect to  $(x, f)$ , then so is  $\gamma'$ .

The following definition is crucial to the proof. Intuitively we use even parts to code  $y_0$  so that we may find a very large stage at which we may witness whether  $\varphi_i(u, v, \beta)$  can be satisfied. However we use the odd parts to indicate when the coding stage is finished.

**Definition 20.7.** Given a finite pair  $(\sigma, \tau) \in T_{\omega_1^\beta}^\beta$ , let  $(x_\sigma, f_\tau) \in [T_{\omega_1^\beta}^\beta[\sigma, \tau]]$  be an infinite path satisfying the following properties:

- If  $f_\tau \smallfrown (n)$  is the least ordinal  $\gamma$  so that  $[T_{\omega_1^\beta}^\beta[x_\sigma \smallfrown n+1, f_\tau \smallfrown n^\frown \gamma]] \neq \emptyset$ ; and
- If  $n$  is the  $2k$ -th number (in the natural ordering sense) for some  $k > 0$  in  $SP_{\sigma, \tau} = \{j \mid (x_\sigma \smallfrown j, f_\tau \smallfrown j) \in [T_{\omega_1^\beta}^\beta[\sigma, \tau]] \text{ is a splitting node}\}$ , then  $x_\sigma(n+1) = x_\sigma(n)^\frown y_0(k)$ ; and
- If  $n$  is the  $2k+1$ -th number for some  $k \geq 0$  in  $SP_{\sigma, \tau}$ , then  $x_\sigma(n+1) = x_\sigma(n)^\frown 0$ .

Obviously given any number  $n$  and pair  $(\sigma, \tau) \in T_{\omega_1^\beta}^\beta$ ,  $(x_\sigma, f_\tau)$  always exists and  $f_\tau \in L_{\max\{\omega_1^\beta, \omega_1^\beta\}}[x]$ .

**Lemma 20.8.**  $\Phi^{x_\sigma}$  codes a well ordering of  $\omega$  with order type  $\beta$ .

*Proof.* Otherwise, by Lemma 20.3,  $x \in L_\beta$ . So by a zig-zag decoding argument over  $T_{\omega_1^\beta}^\beta$ ,  $y_0 \leq x \oplus z_0 \equiv_h z_0$ , a contradiction.  $\square$

**Lemma 20.9.** If there is a pair  $(\sigma, \tau) \in T_{\omega_1^\beta}^\beta$  and some stage  $\gamma < \omega_1^\beta$  so that for any  $n$ ,  $\gamma$  is correct up to  $n$  respect to  $(x_\sigma, f_\tau)$ , then  $x_\sigma \equiv_h y_0$ .

*Proof.* By the property of  $(x_\sigma, f_\tau)$ ,  $f_\tau \in L_{\omega_1^{x_\sigma}}[x_\sigma]$ . We claim that  $\omega_1^\beta \leq \omega_1^{x_\sigma}$ . Otherwise, by Lemma 20.3,  $x_\sigma \in L_\beta$ . By a zig-zag coding over  $T_\gamma^\beta[\sigma, \tau]$ , we have that  $y_0 \in L_{\omega_1^\beta}[x_\sigma] = L_{\omega_1^\beta}$ , a contradiction to the choice of  $y_0$ .

So  $\gamma < \omega_1^\beta \leq \omega_1^{x_\sigma}$ . Then it is clear that, by a zig-zag decoding over  $T_\gamma^\beta[\sigma, \tau]$ , we may decode  $y_0$  by  $(x_\sigma, f_\tau)$ . So  $y_0 \leq_h x_\sigma$ . Obviously  $y_0 \geq_h x_\sigma$ . So  $x_\sigma \equiv_h y_0$ .  $\square$

So if the assumption of Lemma 20.9 holds, then the proof of Theorem 20.1 is finished.

From now on, we assume for any pair  $(\sigma, \tau) \in T_{\omega_1^\beta}^\beta$  and any ordinal  $\gamma < \omega_1^\beta$ , there is some number  $n$  so that  $\gamma$  is not correct up to  $n$  respect to  $(x_\sigma, f_\tau)$ .

Now we turn to the real construction. We will construct an infinite path  $(x, f) \in T_{\omega_1^\beta}^\beta$  so that  $y_0 \equiv_h x$ . To code  $y_0$ , we use a zig-zag coding which is performed in  $L_{\omega_1^\beta+1}$ . So the point is show  $\omega_1^x > \omega_1^\beta$ .

We start to construct  $(x, f)$  by induction on  $\omega$ .

At stage 0. Let  $(\sigma_0^0, \sigma_0^1) = (\emptyset, \emptyset) \in T_{\omega_1^\beta}^\beta$ .

At stage  $s + 1$ . Suppose that  $(\sigma_s^0, \sigma_s^1) \in T_{\omega_1^\beta}^\beta$  has been constructed so that  $(\sigma_s^0, \sigma_s^1)$  is a splitting node in  $T_{\omega_1^\beta}^\beta$  (Without loss of generality, we may assume that  $(\emptyset, \emptyset)$  is a splitting node in  $T_{\omega_1^\beta}^\beta$ ).

Substage (1): We code  $y_0(s)$  at this substage. Let  $\sigma_{s,1}^0$  be the shortest finite string so that there is a string  $\sigma_{s,1}^1$  such that

- (1)  $(\sigma_{s,1}^0, \sigma_{s,1}^1) \in T_{\omega_1^\beta}^\beta$  is a splitting node; and
- (2)  $\sigma_{s,1}^0 \succeq (\sigma_s^0) \frown y_0(s)$ ; and
- (3)  $(\sigma_{s,1}^0, \sigma_{s,1}^1)$  is the leftmost string in  $\{(\sigma_{s,1}^0, \tau) \mid (\sigma_{s,1}^0, \tau) \in T_{\omega_1^\beta}^\beta\}$ .

Obviously such a pair  $(\sigma_{s,1}^0, \sigma_{s,1}^1)$  exists.

Substage(2): We try to make sure  $\omega_1^x > \omega_1^\beta$  at this stage. Let  $(x_{\sigma_{s,1}^0}, f_{\sigma_{s,1}^1}) \in T_{\omega_1^\beta}^\beta[\sigma_{s,1}^0, \sigma_{s,1}^1]$  be as defined in Definition 20.7.

Case(2.1).  $L_{\omega_1^\beta} \models \forall u < \beta \exists v \varphi_i(u, v, \beta)$ . Then let  $\gamma_s$  be the least ordinal so that  $\forall u < \beta \exists v \in L_{\gamma_s} \varphi_i(u, v, \beta)$ . Then by the assumption, we may let  $n_s$  be the least number  $n$  so that

- $(x_{\sigma_{s,1}^0} \upharpoonright n, f_{\sigma_{s,1}^1} \upharpoonright n)$  is a splitting node in  $T_{\omega_1^\beta}^\beta$ ; and
- $n$  is the  $2k+1$ -th number for some  $k \geq 0$  in  $SP_{\sigma_{s,1}^0, \sigma_{s,1}^1} = \{j \mid (x_{\sigma_{s,1}^0} \upharpoonright j, f_{\sigma_{s,1}^1} \upharpoonright j) \in T_{\omega_1^\beta}^\beta[\sigma_{s,1}^0, \sigma_{s,1}^1] \text{ is a splitting node}\}$ ;
- $\gamma_s$  is not correct up to  $n$  respect to  $(x_{\sigma_{s,1}^0}, f_{\sigma_{s,1}^1})$ .

Then let  $(\sigma_{s+1}^0, \sigma_{s+1}^1)$  be a finite string such that

- (1)  $(\sigma_{s+1}^0, \sigma_{s+1}^1) \in T_{\omega_1^\beta}^\beta$  is a splitting node extending  $(x_{\sigma_{s,1}^0} \upharpoonright n_s, f_{\sigma_{s,1}^1} \upharpoonright n_s)$ ; and
- (2)  $\sigma_{s+1}^0 \succeq x_{\sigma_{s,1}^0} \upharpoonright n_s \hat{\ } 1$  (we use this to indicate the coding construction at this stage is finished); and
- (3)  $(\sigma_{s+1}^0, \sigma_{s+1}^1)$  is the leftmost string satisfying above property.

Case(2.2). Otherwise. Then there is some  $u < \beta$  so that  $L_{\omega_1^\beta} \models \forall v \neg \varphi_i(u, v, \beta)$ .

Then by the assumption, let  $n_s$  be the least number  $n$  so that

- $(x_{\sigma_{s,1}^0} \upharpoonright n_s, f_{\sigma_{s,1}^1} \upharpoonright n)$  is a splitting node in  $T_{\omega_1^\beta}^\beta$ ; and

- There is some  $d \in \text{Dom}(\Phi^{x_{\sigma_{s,1}^0} \upharpoonright n})$  so that  $f_{\sigma_{s,1}^1} \upharpoonright n(d) = u$  (remember that  $f_{\sigma_{s,1}^1} \upharpoonright n$  is a finite order preserving function from  $\text{Dom}(\Phi^{x_{\sigma_{s,1}^0} \upharpoonright n})$  to  $\beta$ ); and
- $n$  is the  $2k + 1$ -th number for some  $k \geq 0$  in  $SP_{\sigma_{s,1}^0, \sigma_{s,1}^1}$ ;

Since  $\Phi^{x_{\sigma_{s,1}^0}}$  codes a well ordering of order type  $\beta$ , such a number  $n_s$  must exist.

Then let  $(\sigma_{s+1}^0, \sigma_{s+1}^1)$  be a finite string such that

- (1)  $(\sigma_{s+1}^0, \sigma_{s+1}^1) \in T_{\omega_1^\beta}^\beta$  is a splitting node extending  $(x_{\sigma_{s,1}^0} \upharpoonright n_s, f_{\sigma_{s,1}^1} \upharpoonright n_s)$ ; and
- (2)  $\sigma_{s+1}^0 \succeq x_{\sigma_{s,1}^0} \upharpoonright n_s \hat{1}$  (we use this to indicate the coding construction at this stage is finished); and
- (3)  $(\sigma_{s+1}^0, \sigma_{s+1}^1)$  is the leftmost string satisfying above property.

This finishes the coding construction at stage  $s + 1$ .

Let

$$(x, f) = \bigcup_{s \in \omega} (\sigma_s^0, \sigma_s^1).$$

By the construction,  $f$  is an automorphism between  $\Phi^x$  and an initial segment of  $\omega_1^x$ . By the same proof of Lemma 20.8,  $\Phi^x$  codes a well ordering of  $\omega$  with order type  $\beta$  and so  $\omega_1^x \geq \omega_1^\beta$ . Hence  $f$  is an automorphism between  $\Phi^x$  and  $\beta$ .

We use a method in [44] to decode the coding construction. We shall  $x$ -hyperarithmetically construct an increasing sequence ordinals  $\{\alpha_i\}_{i \in \omega}$  so that  $\lim_i \alpha_i = \omega_1^\beta$ . Then  $\omega_1^x > \omega_1^\beta$ . Once this is archived, then by a zig-zag decoding, we have that  $x \geq_h y_0$  and so  $x \equiv_h y_0$ .

**Definition 20.10.** Given a finite increasing sequence  $\{n_i\}_{i \leq s}$  for some  $s$  and an ordinal  $\gamma < \omega_1^\beta$ , we say that  $\gamma$  *matches*  $\{n_i\}_{i \leq s}$  if all the following facts hold:

- $n_0 = 0$ ; and
- For any  $l \leq n_s$ ,  $(x \upharpoonright l, f \upharpoonright l)$  is the leftmost in  $\{(x \upharpoonright l, \tau) \mid (x \upharpoonright l, \tau) \in T_\gamma^\beta\}$ ; and
- For any  $j \in (0, s]$ ,
  - There is a number  $l_0$  which is the least number greater than  $n_{j-1}$  so that  $(x \upharpoonright l_0, f \upharpoonright l_0)$  is splitting node in  $T_\gamma^\beta$ ; and
  - $(x \upharpoonright l_0, f \upharpoonright l_0)$  is the leftmost finite string in  $\{(x \upharpoonright l_0, \tau) \mid (x \upharpoonright l_0, \tau) \in T_\gamma^\beta\}$ ; and
  - There is a number  $l_1 > l_0$  so that  $(x \upharpoonright l_1, f \upharpoonright l_1)$  is the  $2k + 1$ -th number, for some  $k$ , in  $SP_{x \upharpoonright l_0, f \upharpoonright l_0} = \{j \mid (x \upharpoonright j, f \upharpoonright j) \in T_\gamma^\beta[x \upharpoonright l_0, f \upharpoonright l_0]\}$  is a splitting node so that  $x \succ x \upharpoonright l_1 \hat{1}$ ; and
  - Either  $L_{\omega_1^\beta} \models \forall u < \beta \exists v \in L_\gamma \varphi_{i-1}(u, v, \beta)$  or there is some  $d \in \text{Dom}(\Phi^{x \upharpoonright l_1})$  so that  $L_{\omega_1^\beta} \models \forall v \in L_\gamma \neg \varphi_{i-1}(f(d), v, \beta)$ ; and
  - $n_j$  is the least number greater than  $l_1$  so that  $(x \upharpoonright n_j, f \upharpoonright n_j)$  is a splitting node in  $T_\gamma^\beta$ .

Intuitively if  $\gamma$  matches  $\{n_i\}_{i \leq s}$ , then, up to  $n_s$ ,  $T_\gamma^\beta$  is “quite like  $T_{\omega_1^\beta}^\beta$  along  $(x, f)$ ”.

Now we start to do the decoding construction.

At stage 0, let  $\alpha_0 = 0$  and  $n_0^0 = 0$ . Claim that 0 is inactive,  $i$  is active and  $n_i^0$  is undefined for any  $i > 0$ .

At stage  $s+1$ , then  $i_s$  is the least  $i$  so that  $i$  is active. Also, by induction,  $n_j^s$  is defined for any  $j < i_s$ .

Case(1). There is a number  $i' < i_s$  so that  $\alpha_s + 1$  does not match  $\{n_j\}_{j \leq i'}$ . Let  $i_{s+1}$  be the least such  $i'$ . Let  $\alpha_{s+1} = \alpha_s + 1$  and claim  $i_j$  is active and  $n_j^{s+1}$  is undefined for all  $j \geq i_{s+1}$ . Moreover, set  $n_j^{s+1} = n_j^s$  for any  $j < i_{s+1}$ . Go to next stage.

Case(2). Otherwise. Search an ordinal  $\gamma > \alpha_s$  less than  $\omega_1^\beta$  and a corresponded unique natural number  $n > \max\{n_j^s \mid j < i_s\}$  so that  $\gamma$  matches the finite sequence  $\{n_j^s\}_{j < i_s} \cup \{n\}$ . If during the search, we found an ordinal  $\gamma'$  so that there is a number  $i' < i_s$  so that  $\gamma$  does not match  $\{n_j\}_{j \leq i'}$ . Then do the action as in Case(1). In other words, let  $i_{s+1}$  be the least such  $i'$ . Let  $\alpha_{s+1} = \gamma'$  and claim  $j$  is active and  $n_j^{s+1}$  is undefined for all  $j \geq i_{s+1}$ . Moreover, set  $n_j^{s+1} = n_j^s$  for any  $j < i_{s+1}$ . Go to next stage. Otherwise, by the construction of  $(x, f)$ , there must be such  $\gamma$  and  $n$ . Find the least such  $\gamma$  and the corresponded  $n$ . Let  $\alpha_{s+1} = \gamma$  and  $i_{s+1} = i_s + 1$ . Claim  $j$  is active and  $n_j^{s+1}$  is undefined for all  $j \geq i_{s+1}$ . Moreover, set  $n_j^{s+1} = n_j^s$  for any  $j < i_s$ ,  $n_{i_s}^{s+1} = n$  and claim that  $i_s$  is inactive. Go to next stage.

This finishes the construction at stage  $s+1$ .

Let

$$\theta = \bigcup_{s \in \omega} \alpha_s.$$

**Lemma 20.11.** *For any  $i$ , there is some  $s$  so that for any  $t \geq s$ ,  $n_i^t$  is defined,  $n_i^t = n_i^s$  and  $i$  is inactive at stage  $t$  for any  $t \geq s$ .*

*Proof.* Suppose not. Let  $i$  be the largest number ( $i$  could be 0) so that there is some  $s$  so that for any  $t \geq s$ ,  $n_i^t$  is defined and  $n_i^t = n_i^s$  for any  $t \geq s$ . Then there is an increasing sequence  $\{s_j\}_{j \in \omega}$  so that  $i_{s_j} = i+1$  and  $s_j > s$  for any  $j$ . Note that, by the construction, at stage  $s_j+1$ ,  $n_{i+1}^{s_j}$  is defined and in the tree  $T_{\alpha_{s_j+1}}^\beta[x \restriction n_i^{s_j+1}, f \restriction n_i^{s_j+1}]$ ,  $(x \restriction n_{i+1}^{s_j+1}, f \restriction n_{i+1}^{s_j+1})$  turns to right at most twice. In other words, there are at most two numbers  $l_0 < l_1 \in (n_i^{s_j+1}, n_{i+1}^{s_j+1})$  so that both  $(x \restriction l_0, f \restriction l_0)$  and  $(x \restriction l_1, f \restriction l_1)$  are splitting nodes in  $T_{\alpha_{s_j+1}}^\beta[x \restriction n_i^{s_j+1}, f \restriction n_i^{s_j+1}]$  such that  $x \succ x \restriction l_0^{\frown} 1$  and  $x \succ x \restriction l_1^{\frown} 1$ . Moreover,  $l_1$  is the largest number less than  $n_{i+1}^{s_j+1}$  so that  $(x \restriction l_1, f \restriction l_1)$  is a splitting node in  $T_{\alpha_{s_j+1}}^\beta[x \restriction n_i^{s_j}, f \restriction n_i^{s_j}]$ . Since  $i+1$  is activated at  $s_{j+1}$ ,  $\alpha_{s_j}$  does not match  $\{n_k^{s_j+1}\}_{k \leq i+1}$ . Then either  $(x \restriction l_1, f \restriction l_1)$  is not a splitting node in  $T_{\alpha_{s_j+1}}^\beta[x \restriction n_i^{s_j+1}, f \restriction n_i^{s_j+1}]$  or there exists some  $d \in \Phi^{x \restriction n_{i+1}^{s_j+1}}$  such that  $L_{\omega_1^\beta} \models \forall v \in L_{\alpha_{s_j}} \neg \varphi_i(f(d), v, \beta)$  but  $L_{\omega_1^\beta} \models \exists v \in L_{\alpha_{s_j+1}} \varphi_i(f(d), v, \beta)$ . In either case, the finite string  $(x \restriction$

$l_1^{\cap} 0, \tau)$  will be cut off from  $T_{\alpha_{s_j+1}}^{\beta}[x \restriction n_i^{s_j+1}, f \restriction n_i^{s_j+1}]$ . But this happens for every  $j$ , so it is clear that  $(x, f)$  must be the leftmost infinite path in  $T_{\theta}^{\beta}[x \restriction k, f \restriction k]$  for some fixed  $k \geq n_i^s$ . Then  $(x, f)$  is the leftmost infinite path in  $T_{\omega_1^{\beta}}^{\beta}[x \restriction k, f \restriction k]$ , which contradicts our construction of  $(x, f)$  (since  $y(i) = 1$  for infinitely many  $i$ 's).  $\square$

**Lemma 20.12.** *For any  $i$ , there must be some  $s$  and  $d \in \text{Dom}(\Phi^{x \restriction n_{i+1}^s})$  so that for any  $t \geq s$ , either  $L_{\omega_1^{\beta}} \models \forall u < \beta \exists v \in L_{\alpha_s} \varphi_i(u, v, \beta)$  or  $L_{\omega_1^{\beta}} \models \forall v \in L_{\alpha_t} \neg \varphi_i(f(d), v, \beta)$*

*Proof.* By Lemma 20.11, there is some  $s$  so that for any  $t \geq s$ ,  $n_i^t$  is defined,  $n_i^t = n_i^s$  and  $i$  is inactive at stage  $t$  for any  $t \geq s$ . Then at stage  $s$ , either  $L_{\omega_1^{\beta}} \models \forall u < \beta \exists v \in L_{\alpha_s} \varphi_i(u, v, \beta)$  or there is some  $d \in \text{Dom}(\Phi^{x \restriction n_{i+1}^s})$  such that  $L_{\omega_1^{\beta}} \models \forall v \in L_{\alpha_s} \neg \varphi_i(f(d), v, \beta)$ . If the first case happens, then we finishes the proof. Otherwise, since  $i$  is never activated from stage  $s$  and  $\text{Dom}(\Phi^{x \restriction n_{i+1}^s})$  is finite, there must be some fixed  $d \in \text{Dom}(\Phi^{x \restriction n_{i+1}^s})$  so that  $L_{\omega_1^{\beta}} \models \forall v \in L_{\alpha_t} \neg \varphi_i(f(d), v, \beta)$ .  $\square$

So by Lemma 20.12,  $\theta \geq \omega_1^{\beta}$  and so  $\theta = \omega_1^{\beta}$ .

This completes the proof of Theorem 20.1.

**Remark:** This argument can be pushed up to prove Friedman's conjecture for  $\Delta_3^1$ -sets and answer several questions in [26] for level 3. Then by recent work of Yizheng Zhu, we believe those questions can be answered fully.

## Part 9. Model theory and definability

### 21. DESCRIPTIONS IN SECOND ORDER LOGIC

The following is a result of Hyttinen, Kangas and Väänänen [24, Thm. 3.3]. It shows that under the right hypothesis on a cardinal  $\kappa$ , the models of a countable complete theory that have size  $\kappa$  can be described in second order logic iff the theory is easy in the sense of Shelah's main gap.

**Theorem 21.1** ([24]). *Let  $T$  be a countable complete theory. For every infinite cardinal  $\kappa$  with  $\kappa = \aleph_{\alpha}$ , where  $\beth(|\alpha| + \omega_1) < \kappa$  and  $2^{\lambda} < 2^{\kappa}$  for each  $\lambda < \kappa$ , the following are equivalent:*

- (i) *Every model of  $T$  of size  $\kappa$  has a description in  $L_{\kappa, \omega}^2(T)$ .*
- (ii)  *$T$  is superstable, shallow, fails the dimensional order property DOP and fails the omitting types order property OTOP.*

Explanations:  $L_{\kappa, \omega}^2(T)$  is the second-order language over the symbol set of  $T$  with disjunctions of size  $< \kappa$  and finite strings of quantifiers.

Superstability of  $T$  is stronger than stability: no infinite linear order can be defined in a model of  $T$  using a formula in  $L_{\omega_1, \omega}$  with parameters. Shelah proved that a model of a theory  $T$  without DOP can be thought of as built from a tree of small models. Shallowness of  $T$  means that for each model of  $T$ , this tree has no infinite path.

## 22. KOLEZHITSKIY: ROBINSON'S THEOREM THAT $\mathbb{Z}$ IS DEFINABLE IN $\mathbb{Q}$

Yan Kolezhitskiy and André Nies discussed a celebrated result of Julia Robinson as part of a semester reading project. The result was originally obtained as part of her 1948 PhD thesis under the supervision of Alfred Tarski. It then appeared in the 1949 J.Symb. Logic [39]. Much simpler formulas for defining  $\mathbb{Z}$  in  $\mathbb{Q}$  have been obtained in subsequent work: a  $\Pi_2$  by Poonen, and recently a  $\Pi_1$  by Jochen Koenigsmann. If  $\mathbb{Z}$  was also  $\Sigma_1$  definable in  $\mathbb{Q}$  then the existential theory of  $\mathbb{Q}$  would be undecidable, which is an open problem at present.

**Theorem 22.1** ([39]). *The set of integers is definable without parameters in the field of rationals  $(\mathbb{Q}, +, \times, 0, 1)$ .*

**Idea and structure of the proof.** A subset  $S$  of  $\mathbb{Q}$  is called *inductive* if  $0 \in S$  and  $y \in S \rightarrow y + 1 \in S$  for each  $y$ . The following is a monadic *second-order* definition of  $\mathbb{N}$  in  $\mathbb{Q}$ :

$$(22.1) \quad k \in \mathbb{N} \Leftrightarrow \forall S [S \text{ is inductive} \rightarrow k \in S].$$

Julia's idea was that it suffices to quantify over a small collection of sets  $S$ , which is uniformly parameterised by pairs of rationals  $a, b$ . Let

$$(22.2) \quad \phi(a, b, k) \equiv \exists x \exists y \exists z (2 + abk^2 + bz^2 = x^2 + ay^2)$$

She used some number theory to show that the sets  $S_{a,b}$  of the form  $\{k: \mathbb{Q} \models \phi(a, b, k)\}$  suffice.

We can now turn the universal second-order quantification over  $S$  into a universal quantification over rationals  $a, b$  in order to obtain a first-order definition replacing (22.1):

$$(22.3) \quad k \in \mathbb{N} \Leftrightarrow \forall a \forall b [S_{a,b} \text{ is inductive} \rightarrow k \in S_{a,b}].$$

Clearly, with a smaller collection of sets  $S$  the implication from left to right in (22.3) still holds. The worry is that we don't have enough sets any longer to separate a rational not in  $\mathbb{N}$  from  $\mathbb{N}$ . (We note that Julia actually only manages to separate non-integer rationals from  $\mathbb{N}$ ; a small complication of to the idea outlined above will be needed for that. She in effect first defines a set  $V$  in between  $\mathbb{N}$  and  $\mathbb{Z}$ , then notes that  $\mathbb{Z} = V \cup -V$ .)

We have to pick the condition  $\phi(a, b, k)$  wisely, ensuring that the relevant sets  $S_{a,b}$  are inductive. This is done via the following fact. We say that  $k = n/d$  in its lowest terms, if  $n \in \mathbb{Z}$ ,  $d \in \mathbb{N} - \{0\}$  and  $(n, d) = 1$ . We also say that  $d$  is the denominator of  $k$  in its lowest terms.

**Fact 22.2.** *Let  $S$  be a set of rationals given by a condition that holds for 0 and only depends on the denominator of the rational in lowest terms. Then  $S$  is inductive.*

The fact is evident because a rational  $q$  has the same denominator in lowest terms as  $q + 1$ .

Next she shows that for two particular kinds of choices for  $a, b$ , the condition  $\phi(a, b, k)$  in (22.2) only depends on the denominator of  $k$  in its lowest terms. Firstly,  $b$  is a prime  $p$  such that  $p \equiv 3 \pmod{4}$ , and  $a = 1$ .

**Lemma 22.3.** *Suppose that  $p$  is a prime such that  $p \equiv 3 \pmod{4}$ . The equation  $2 + pk^2 + pz^2 = x^2 + y^2$  has a solution for  $x$ ,  $y$ , and  $z$  iff the denominator of  $k$  in its lowest terms is odd, and is co-prime to  $p$ .*

Secondly,  $a$  is a prime  $q$  and  $b$  is a prime  $p$ , with some additional restrictions. Recall that the Legendre “symbol”  $(k/p)$  is a binary function that returns 1 if  $k$  is a quadratic residue  $\text{mod } p$ , 0 if  $k = 0$ , and  $-1$  otherwise.

**Lemma 22.4.** *Suppose that  $p$  and  $q$  are odd primes such that  $p \equiv 1 \pmod{4}$  and  $(q/p) = -1$ . The equation  $2 + pqk^2 + pz^2 = x^2 + qy^2$  has a solution for  $x$ ,  $y$ , and  $z$  iff the denominator of  $k$  in its lowest terms is co-prime to both  $q$  and  $p$ .*

Given these two lemmas, the proof concludes as follows. First one needs a number theoretic claim which provides the  $q$  we need in Lemma 22.4.

**Claim 22.5.** *Suppose  $p$  is a prime such that  $p \equiv 1 \pmod{4}$ . There exists an odd prime  $q$  such that  $(q/p) = -1$ .*

*Proof.* Let  $s$  be any (quadratic) non-residue  $\text{mod } p$ . Then  $s + p$  is also a non-residue. One of  $s$ ,  $s + p$  is odd, say the former. There is an (odd) prime factor of  $s$  which is also a non-residue, because the Legendre symbol is multiplicative. Let this prime factor be  $q$ .  $\square$

Let  $\psi(k)$  be a first-order formula expressing the right hand side of (22.3). Clearly  $k \in \mathbb{N} \Rightarrow \psi(k)$ . We verify that  $\psi(k) \Rightarrow k \in \mathbb{Z}$ . Suppose that  $k \in \mathbb{Q}$  and  $\psi(k)$  holds. Write  $k = n/d$  in lowest terms. By Lemma 22.3,  $d$  is odd and not divisible by any prime  $p$  such that  $p \equiv 3 \pmod{4}$ . By Lemma 22.4 using Claim 22.5,  $d$  not divisible by any prime  $p$  such that  $p \equiv 1 \pmod{4}$ . Therefore  $d = 1$ .

Thus,  $k \in \mathbb{N} \Rightarrow \psi(k) \Rightarrow k \in \mathbb{Z}$ , so the formula  $\psi(k) \vee \psi(-k)$  provides a first-order definition of  $\mathbb{Z}$  in  $\mathbb{Q}$ .

**Proofs of Lemmas 22.3 and 22.4.** Julia relies on two claims that follow from the Hasse-Minkowski theorem.

**Claim 22.6.** *Suppose  $p$  is a prime such that  $p \equiv 3 \pmod{4}$ . We have  $x^2 + y^2 - pz^2 = m$  for some  $m \in \mathbb{Q}$ ,  $m \neq 0$ , iff it is not the case that*

- a)  $m = pks^2$ , where  $(k/p) = 1$ , or
- b)  $m = ks^2$  with  $k \equiv p \pmod{8}$

**Claim 22.7.** *Suppose  $p$  and  $q$  are odd primes such that  $p \equiv 1 \pmod{4}$  and  $(q/p) = -1$ . There is some non-zero  $m \in \mathbb{Q}$  such that  $x^2 + qy^2 - pz^2 = m$ , iff it is not the case that:*

- a)  $m = pks^2$  and  $(k/p) = -1$
- b)  $m = qks^2$  and  $(k/q) = -1$



## REFERENCES

- [1] Uri Andrews, Mingzhong Cai, David Diamondstone, Carl Jockusch, and Steffen Lempp. Asymptotic density, computable traceability, and 1-randomness. Preprint, 2013. [4](#)
- [2] L. Bienvenu, P. Gács, M. Hoyrup, C. Rojas, and A. Shen. Algorithmic tests and randomness with respect to a class of measures. *Proceedings of the Steklov Institute of Mathematics*, 274(1):34–89, 2011. Published in Russian in *Trudy Matematicheskogo Instituta imeni V.A. Steklova*, 2011, Vol. 274, pp. 41–102. [18](#)
- [3] L. Bienvenu, N. Greenberg, A. Kučera, A. Nies, and D. Turetsky. Coherent randomness tests and computing the K-trivial sets. To appear in J. European Math. Society, 2016. [3.1](#), [3.1](#), [3.6](#), [8](#), [9](#)
- [4] Andreas Blass. Some questions arising from hindman’s theorem. *Scientiae Mathematicae Japonicae*, (62):331–334, 2005. [10](#)
- [5] J. Brendle, A. Brooke-Taylor, Keng Meng Ng, and A. Nies. An analogy between cardinal characteristics and highness properties of oracles. In *Proceedings of the 13th Asian Logic Conference: Guangzhou, China*, pages 1–28. World Scientific, 2013. <http://arxiv.org/abs/1404.2839>. [7](#)
- [6] Yue Yang Chi Tat Chong, Steffen Lempp. On the role of the collection principle for  $\sigma_2^0$  formulas in second-order reverse mathematics. *Proceedings of the American Mathematical Society*, 138:1093–1100, 2010. [10](#)
- [7] Yue Yang Chi Tat Chong, Theodore Slaman. The metamathematics of the stable ramsey’s theorem for pairs. *Journal of the American Mathematical Society*, 27:863–892, 2014. [10](#)
- [8] Barbara F Csima and Joseph R Mileti. The strength of the rainbow Ramsey theorem. *The Journal of Symbolic Logic*, 74(04):1310–1324, 2009. [8](#), [9](#)
- [9] Jeff Hirst Damir Dzhafarov. The polarized ramsey’s theorem. *Archive for Mathematical Logic*, 48(2):141–157, 2009. [10](#), [10](#), [10](#), [10](#)
- [10] Reed Solomon Linda B. Westrick Damir Dzhafarov, Carl G. Jockusch. Effectiveness of hindman’s theorem for bounded sums. In N. Greenberg B. Khoussainov A. Melnikov A. Day, M. Fellows, editor, *Proceedings of the International Symposium on Computability and Complexity (in honour of Rod Downey’s 60th birthday)*, Lecture Notes in Computer Science. Springer, To appear. [10](#), [10](#), [10](#), [10](#), [1](#), [10](#)
- [11] A. Nies (editor). Logic Blog 2013. Available at <http://arxiv.org/abs/1403.5719>, 2013. [8](#), [9](#)
- [12] A. Nies (editor). Logic Blog 2015. Available at <http://arxiv.org/abs/1602.04432>, 2015. [4](#), [6](#)
- [13] S. Figueira, D. Hirschfeldt, J. Miller, Selwyn Ng, and A Nies. Counting the changes of random  $\Delta_2^0$  sets. *J. Logic Computation*, 25:1073–1089, 2015. Journal version of conference paper at CiE 2010. [8](#), [8](#), [9](#), [9](#)
- [14] Santiago Figueira, Joseph S. Miller, and André Nies. Indifferent sets. *J. Logic Comput.*, 19(2):425–443, 2009. [2](#)
- [15] M. Fried and M. Jarden. *Field arithmetic*, volume 11. Springer Science & Business Media, 2006. [17.5](#), [17.1](#), [17.6](#), [17.2](#), [17.2](#), [17.15](#), [17.2](#)
- [16] Su Gao. *Invariant descriptive set theory*, volume 293 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2009. [14](#)
- [17] Su Gao, S. Jackson, and B. Seward. *Group colorings and Bernoulli subflows*, volume 241. American Mathematical Society, 2016. [19](#)
- [18] D. Gorenstein, R. Lyons, and R. Solomon. *The classification of the finite simple groups 3*, volume 40. American Mathematical Soc., 1998. [15](#)
- [19] Alexandre Grothendieck. Résumé de la théorie métrique des produits tensoriels topologiques. *Resenhas do Instituto de Matemática e Estatística da Universidade de São Paulo*, 2(4):401–481, 1996. This is a reprint of a 1953 paper. [13](#)
- [20] R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky. Presentations of finite simple groups: a quantitative approach. *J. Amer. Math. Soc.*, 34:711–774, 2008. [15](#)

- [21] Leo A. Harrington. Analytic determinacy and  $0^\#$ . *J. Symbolic Logic*, 20:685–693, 1978. [20](#), [20.1](#)
- [22] M. Hoyrup and C. Rojas. Computability of probability measures and Martin-Löf randomness over metric spaces. *Inform. and Comput.*, 207(7):830–847, 2009. [18](#)
- [23] Mathieu Hoyrup and Cristobal Rojas. An Application of Martin-Löf Randomness to Effective Probability Theory. In Klaus Ambos-Spies, Benedikt Löwe, and Wolfgang Merkle, editors, *CiE*, pages 260–269. Springer, 2009. [17.2](#)
- [24] T. Hyttinen, K. Kangas, and J. Väänänen. On second-order characterizability. *Logic Journal of IGPL*, 21(5):767–787, 2013. [21](#), [21.1](#)
- [25] M. Jarden and A. Lubotzky. Random normal subgroups of free profinite groups. *Journal of Group Theory*, 2:213–224, 1999. [17.1](#), [17.7](#)
- [26] Alexander S. Kechris, Donald A. Martin, and Robert M. Solovay. Introduction to  $Q$ -theory. In *Ordinal Definability and Recursion Theory. The Cabal Seminar. Volume III*, volume 43 of *Lect. Notes Log.*, pages 126–199. Cambridge University Press, Cambridge, 2016. [20.2](#)
- [27] Wolfgang Kimmerle, Richard Lyons, Robert Sandling, and David N Teague. Composition factors from the group ring and artin’s theorem on orders of simple groups. *Proceedings of the London Mathematical Society*, 3(1):89–122, 1990. [15](#)
- [28] Donald A. Martin. Proof of a conjecture of Friedman. *Proc. Amer. Math. Soc.*, 55(1):129, 1976. [20.2](#)
- [29] B. Monin and A. Nies. A unifying approach to the Gamma question. In *Proceedings of Logic in Computer Science (LICS)*. IEEE press, 2015. [5](#), [5](#), [5](#)
- [30] A. Nies. Calculus of cost functions. To appear in Barry Cooper and Mariya Soskova (eds.), *The Incomputable: Journeys beyond the Turing barrier*, Springer-Verlag. [3](#)
- [31] A. Nies. *Computability and randomness*, volume 51 of *Oxford Logic Guides*. Oxford University Press, Oxford, 2009. 444 pages. Paperback version 2011. [2](#), [3.2](#), [8](#), [8](#), [9](#), [9](#)
- [32] A. Nies and K. Tent. Describing finite groups by short first-order sentences. *Israel J. of Mathematics*, to appear, 2014, updated 2015. available at arXiv:1409.8390. [15](#), [15](#), [15](#)
- [33] Theodore A. Slaman Peter A. Cholak, Carl G. Jockusch. On the strength of ramsey’s theorem for pairs. *Journal of Symbolic Logic*, 66(1):1–55, 2001. [10](#)
- [34] G. Pisier. Grothendieck’s theorem, past and present. *Bulletin of the American Mathematical Society*, 49(2):237–323, 2012. [13](#)
- [35] Michael O. Rabin. Computable algebra, general theory and theory of computable fields. *Trans. Amer. Math. Soc.*, 95:341–360, 1960. [17.2](#)
- [36] P. Raghavendra and D. Steurer. Towards computing the grothendieck constant. In *Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 525–534. Society for Industrial and Applied Mathematics, 2009. [13](#)
- [37] L. Ribes and P. Zalesskii. *Profinite groups*. Springer, 2000. [17.1](#), [17.4](#), [17.1](#)
- [38] D. Robinson. *A course in the theory of groups*. Springer-Verlag, 1988. [14](#)
- [39] J. Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14(2):98–114, 1949. [22](#), [22.1](#)
- [40] S. G. Simpson. *Subsystems of second order arithmetic*. Perspectives in Logic. Cambridge University Press, Cambridge, second edition, 2009. [18](#)
- [41] R. Smith. Effective aspects of profinite groups. *The Journal of Symbolic Logic*, 46(04):851–863, 1981. [17.8](#)
- [42] S. Thomas. Topological full groups of minimal subshifts and just-infinite groups. In *Proceedings of the 12th Asian Logic Conference*, pages 298–313. World Scientific, 2013. [19](#)
- [43] Ingo Wegener et al. *The complexity of Boolean functions*, volume 1. BG Teubner Stuttgart, 1987. [11](#)
- [44] Liang Yu. A new proof of Friedman’s conjecture. *Bull. Symbolic Logic*, 17(3):455–461, 2011. [20.2](#)